Intelligent Biology

From Control to Influence:

Cognition in the Grey Zone

Report for the Pentagon Joint Staff Strategic Multilayer Assessment Group

Nicholas D. Wright

– v3 Jan 2019 –

A FAMILY OF PRODUCTS TO CREATE INFLUENCE IN THE GREY ZONE

This report is part of a coherent family of products that together provide a framework for successful influence in the Grey Zone. All are available from www.nicholasdwright.com. These include:

Principles of Grey Zone influence:
- Wright, ND (2019) *From Control to Influence: Cognition in the Grey Zone,* Intelligent Biology.

Outer space Grey Zone competition:
- Wright, ND (2019) *MindSpace: Cognition in space operations,* Intelligent Biology.
- Ed. Wright, ND (2018) *Outer Space; Earthly Escalation? Chinese Perspectives on Space Operations and Escalation,* U.S. Dept. of Defense Joint Staff.

North Korea and Grey Zone competition:
- Wright, ND (2018) *Getting Messages Through: The cognition of influence with North Korea and East Asia,* Intelligent Biology.

Artificial Intelligence in the global competition for influence:
- Ed. Wright ND, (2018) *AI, China, Russia and the Global Order*: *Technological, Political, Global, and Creative Perspectives,* U.S. Dept. of Defense Joint Staff.

About the author

Dr Nicholas Wright is affiliated with Georgetown University, University College London (UCL), Intelligent Biology and New America. His work combines neuroscientific, behavioural and technological insights to understand decision-making in politics and international confrontations, in ways practically applicable to policy. He regularly works with Governments. He has numerous academic and general publications. He received a medical degree from UCL, a BSc in Health Policy from Imperial College London, has Membership of the Royal College of Physicians (UK), has an MSc in Neuroscience and a PhD in Neuroscience both from UCL.

TABLE OF CONTENTS

Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF BOXES

EXECUTIVE SUMMARY

Understanding and influencing adversary decision-making in Grey Zones requires anticipating key audiences' perceptions and decision-making. We apply evidence from the neuroscience and psychology of human decision-making to help policymakers produce intended and avoid unintended effects in the Grey Zone.

Key features of the Grey Zone: the centrality of influence

Grey Zone conflict is necessarily *limited* conflict, sitting between "normal" competition between states and what is traditionally thought of as war. Thus, the central aim is to *influence* the decision-making of adversaries and other key audiences, rather than removing their capacity to choose using brute force in itself. Success requires moving the emphasis from control to influence.

What, if anything, differentiates the Grey Zone from other types of conflict? The fundamental nature of conflict is unchanged, but the Grey Zone requires different *emphases*. I summarise these key challenges as the *"Five Multiples"* of the Grey Zone.

(1) Multiple levels: The U.S. must successfully influence multiple societal levels, namely at the *state level* (e.g. adversarial, allied or neutral states); at the *population level* (e.g. mass communication within states and communities); and at the *non-state actor level* (e.g. proxies, violent extremist organisations or quasi-states like Da'esh).

We systematically evaluate empirical, real-world evidence to identify key cognitive factors for influence multiple levels. We integrate these into usable tools. For example, a "*Checklist for empathy*" (Box 2.1) provides a realistic analysis of an adversary, ally and other's decision calculus. This includes key human motivations such as fairness, legitimacy, surprise and self-interest.
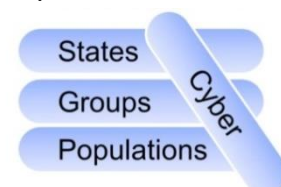
(2) Multiple domains and instruments of power: Multiple domains—e.g. military, information, economic and cyber—cut across these multiple societal levels.

Key cognitive factors can be common or differ between domains. For instance, managing surprise and predictability (concepts incorporated in a simple *"prediction error" framework* grounded in neuroscience; Chapters 4, 5, 7 and 8) is critical across domains and levels to cause intended effects and avoid unintended effects.

(3) Multiple timeframes: One must consider at least two separate timeframes: managing an ongoing process evolving over years; and managing short-term crises in light of that ongoing process.

Combating propaganda, conducting information operations and messaging more generally at all societal levels critically involves messengers that are trusted and credible to the target

audience. Trust is fundamentally psychological, and trusted messengers can often only be created over longer timeframes (e.g. the BBC).

Consider the two biggest historical cases of inadvertent escalation between European powers since 1815: the road to the Crimean War of 1854 in which some 800,000 soldiers died in the Anglo-French versus Russian conflict; and road to the First World War. Both were preceded by lengthy Grey Zone confrontations involving multiple episodes. Policy-makers must be aware that each episode in the Grey Zone sets the stage for the next interaction. Violating norms, even for admirable reasons, can escalate Grey Zone conflict on a longer timeframe.

(4) Multiple audiences: Ally and third party perceptions are critical in the Grey Zone – and U.S. actions will inevitably reach multiple audiences. For instance, if it lost allied support in the South China Sea, the U.S could suffer deterrence by ally denial.

Audience analysis is critical across these multiple audiences. This requires both local knowledge within key local audiences, and also the ability of the U.S. analysts to put themselves in the shoes of their audiences – the type of "outside-in" thinking enabled by our *Checklist for Empathy*.

(5) Multiple interpretations: Ambiguity is a key feature of the Grey Zone. Ambiguity's essence is that events or actions are open to multiple interpretations. Ambiguity provides an extra layer of uncertainty even before one consider an event's risk, and can thus directly contribute to crisis escalation. Ambiguity can also help de-escalate crises, for example enabling compromises that save face on both sides (e.g. the "apology" in the 2001 Sino-U.S. EP-3 incident). In the long run ambiguous actions can change behavioural norms and thus escalate international tensions.

Report outline

Strategy in the Grey Zone is the art of creating influence. This report's four parts provide a framework for how to create that power:

- Part I provides evidence-based principles for influence in the Grey Zone;
- Part II examines key cognitive factors in the Grey Zone;
- Part III examines cyber in the Grey Zone;
- Part IV describes how to measure influence in the Grey Zone.

This report is one of a coherent family of products that together provide a framework for successful influence in the Grey Zone. Other products examine Grey Zone competition involving Outer Space (Wright, 2019), North Korea (Wright, 2018) and Artificial Intelligence (Wright, 2018). All available at www.nicholasdwright.com.

Part I Principles of Influence in the Grey Zone

Part I provides evidence-based recommendations to make the most of current thinking on techniques for influence. It draws on expertise from multiple sectors—including security,

psychology, neuroscience and the commercial world—and assigns a score for the strength of evidence underlying each recommendation it covers (details of the evidence base are in Appendix 1). It specifically examines evidence to exert influence at the state level and at the population level, as working at *both* levels together is a key challenge in the Grey Zone. For ease of presentation, Part I is divided into three chapters that focus on Audiences; Messages; and then Messengers.

Chapter 2 Audiences

Influence efforts must be tailored to the audience to maximise intended effect. Five key concepts are:

*(1) Organisations should adopt an **"outside-in"** mindset, which makes the audience's decision-making process the focus of the influence strategy.* To influence an Afghan farmer not to grow poppy, or if we seek to deter an adversary state, the influencer must consider that course of action and its alternatives from *their* perspective. We must estimate how they perceive the costs and benefits of acting, or of not acting.

Simple, structured approaches should be used to understand the audience's decision-making process. Many tools are available; the key is to use a structured approach. One such approach is a **"checklist for empathy".**

"Checklist for empathy"

A set of practical questions can help to estimate the audience's perceived costs and benefits for their potential alternative actions in a given context. These may include:

Self-interest: *"What material benefits may they gain or lose?"* The importance of self-interest was shown by the switching allegiances of Sunni groups during the 2007 Surge in Iraq, which involved U.S. rewards and threats of punishment.

Fairness: *"How fair will it be seen from the audiences' perspectives?"* Humans typically pay costs to reject unfairness and pursue grievances.

Fear: "Do they fear for their security and why?"

Identity: *"What are their key identities?"* Humans are driven to form groups ("us", the "in-group") that are contrasted against other groups ("them", the "out-group"). Individuals also often hold multiple overlapping identities.

Status: *"How may this affect the audience's self-perceived status?"* E.g. For key audiences in Afghanistan, joining the Taliban had high status.

Expectations: "*What are their key expectations, and what may violate them?* The more unexpected a perceived event is, the bigger its psychological impact.

Context, opportunity and capability. "*What opportunities and capabilities does the audience perceive it has for its potential alternative actions?"*

---

(2) Messages are likely to reach multiple audiences – so it is vital to anticipate potentially divergent influences.

(3) Audiences seldom passively receive messages. Audience analysis often requires understanding the ongoing, interactive relationship with messengers.

(4) Identify groups with a propensity for influence and who are more likely to act on the influence they encounter. Focus on them and develop specific strategies to influencing them.

(5) Audience analysis is a key area of competition with potential adversaries.
- The Russians are held to conduct good audience analysis, with which the US and allies must be able to compete.
- The Chinese surprisingly are held to conduct little audience analysis – and thus better understanding audiences is a potentially critical US and allied advantage.

As well as the five areas outlined above, Chapter 2 also discusses particular factors that influence audience behavior, such as age.

Chapter 3 Messages

After developing an in depth understanding of the target audience, successful messages must be developed. This chapter discusses how to fashion messages, the content of messages and then the context of messages.

*(1) When **fashioning messages**, consider the following*
- The message must be simple while not leaving an incomplete narrative.
- The audience must find the message sufficiently credible.
- Creativity in messaging is often key – manage novelty and unexpectedness, otherwise messages may lack the salience needed to impact on audiences.

*(2) **Content of messages:** Messages should address key audience motivations such as identity, fairness, fear or self-interest (e.g. see checklist for empathy above).*

*(3) It is vital to consider the **communication context**, not the message content alone.* Humans are attuned to evaluate stimuli by comparing stimuli with other stimuli or options, so use **contrast effects** to make the desired option the better option.
- **Timing matters:** Prepare for influence operations on timescales of minutes (e.g. responding on social media) to years (the Chinese building of Confucius Institutes).
- **Standing out against noise:** Any message's impact is determined partly by the factors set out here and partly by the background volume of all other information an audience receives. 'Noise' can be a strategy. Russia, for instance, rather than promulgating one specific positive explanation of an event, such as the MH17 airliner crash over East Ukraine in 2014, instead created noise by circulating many different (at times contradictory) explanations. Interestingly, this seems in contrast to Chinese techniques, which seek to explain their perspective or narrative and more focus on being understood. *No one clear strategy exists to stand out against noise: it is likely best achieved by audience-centred approaches that use evidence-based techniques to fashion messages, which are delivered by credible messengers.*
- Counter-messaging should be augmented by longer-term, more **preventative interventions**, e.g. television discussion programmes or radio soap operas involving community cohesion. A coherent media strategy should be part of peri-conflict nation- or state-building efforts.

Chapter 4 Messengers

Finding and developing the right messengers is vital. We cover three areas.

Firstly, policy must consider three key messenger characteristics: trust, salience and capability.
   (a) ***Trust*** *in messengers is often critical and is in the eye of the audience.* Multiple factors contribute, including perceived expertise, good intentions and capability. Messengers' similarity to an audience increases influence, as does "liking" of them at the population level and "soft power" at the state level. Governments are often not the most appropriate messenger, which can be overcome by developing partnerships with trusted individuals and groups.
   (b) *Messengers must also be **salient** to audiences, they need to stand out to be able to impact psychologically on audiences constantly bombarded by information.* One way is to manage the **unexpectedness of messengers**. Iranian President Rouhani's unexpected use of 2013 Twitter diplomacy changed the political climate and enabled successful nuclear talks. Repeated exposure to the same messenger can lead audiences to habituate. However, **familiarity** with messengers can also increase their influence. Ambiguity and "salami slicing" can help minimize unexpectedness and avoid adverse responses. Using **multiple messengers** over time enables one to change between them.
   (c) *Messengers must be **capable** of reaching audiences.* Television, radio and social media impact may vary according to audience. **Language** is one critical factor.

*Second, understanding **networks** can help identify effective messengers.* Face-to-face, family, social media and other networks can provide key access to audiences. Three issues for the policy maker are: (a) What are key social networks amongst the audience? (b) What networks link the audience to the outside? Trust exists in networks, so networks can be good messengers to access an audience. (c) Who are key **opinion leaders**?

Third, competition with other actors: Key State and non-State actors place influence at the heart of their activities, invest heavily and stress influence at the highest policy levels.
   (a) *Resources and high-level policy support:* **State competitors** such as Russia and China have been building powerful, well-resourced messenger capabilities. China is investing $7-10 billion per annum. Adversaries like Da'esh can use cheap **asymmetric strategies**, such as social media. To compete, U.S. and allied influence capabilities must have appropriate resources, high-level policy support and cross-government organisational structures that provide strategic level coordination with tactical autonomy, adaptability and responsiveness.
   (b) *Timescales:* Interacting with capable competitors requires preparing for influence on timescales of **minutes,** such as responding to key events on social media and the 24/7 newsfeed. This requires a rapid response set within a strategic plan. At that other end of the scale, is the establishment of institutions such as the BBC, which take **years** to build.
   (c) *Concepts:* Western views of information security fundamentally differ from Russian and Chinese approaches, which are more holistic and cognitive.
   (d) *Agility:* Help organisational flexibility by adopting an **"outside-in"** perspective (Chapter 2), and draw on **external partner organisations** to meet audience needs.

Part II Key Cognitive Factors in the Grey Zone

Part II focusses on four key cognitive aspects of Grey Zone conflict. Chapter 5 examines risk, ambiguity and other aspects of uncertainty. Chapter 6 examines the closely bound human motivations related to fairness, legitimacy, status and honour. Chapter 7 discusses how international norms change. Chapter 8 discusses cognitive aspects of deterrence and escalation management in the Grey Zone.

Chapter 5 Risk, ambiguity and mastering uncertainty

Uncertainty pervades Grey Zone competitions. Uncertainty can be usefully broken down into multiple distinct components that require different policies, in particular risk and ambiguity. Policymakers can manipulate risk, and use it as a tool for deterrence or escalation management. They can also manipulate ambiguity, which is one of the "five multiples of the Grey Zone." Understanding risk *and* ambiguity are key to achieve intended and avoid unintended effects.

Defining risk and ambiguity is highly contentious because multiple overlapping definitions exist across different disciplines. However, the basic concepts are not that confusing. Risk refers situations in which all the probabilities are known; whilst ambiguity refers to those with an extra layer of uncertainty, for instance where some probabilities are unknown.

Ambiguity in international confrontations: Ambiguity in events and actions gives an extra layer of uncertainty, so they are open to *multiple interpretations* before we even consider their risk. An analogy is perceptual ambiguity – does the picture here show an old lady or a young lady?

Cases of managing ambiguity include: (1) Ambiguity is a key tool in diplomacy. The 2001 Sino-US crisis where an EP-3 reconnaissance plane force-landed on Hainan Island was, for instance, resolved by a letter that could be *interpreted* one way by the Chinese for their public, and another by the US for their public. (2) Russian use of "little green men" makes an offensive action more ambiguous and so more easily deniable – e.g. at least for observing populations in key allies even if not for US security analysts. Countering that ambiguity requires US and allied investment in good communication and attribution capabilities ahead of time, which are trusted by key audiences. (3) Ambiguous thresholds for deterrent threats enable less loss of face if they are crossed, e.g. compared to hard "red lines." (4) Concessions are critical to manage escalation, especially with a nuclear-armed adversary – and ambiguity enables deniability, as successfully used between US President Nixon and China's Chairman Mao. (5) Economic actions by possible proxies carry ambiguity, e.g. Chinese companies' investments on key Pacific Islands.

Risk in international confrontations: Risk arises when potential outcomes are uncertain. (1) Consider US, UK and German troops currently deploying to NATO's east, such as the Baltic Republics. Their placement is unambiguous, and provides a tripwire so that there is the risk of escalation if serious aggression occurred. This is a classic use of the risk of escalation, as described by Thomas Schelling who devotes a chapter to the "*Manipulation of*

Risk " in his seminal *Arms and Influence* (1966). He describes how the risk is that escalation can develop its own momentum. (2) Schelling also argues that *"limited war, as a deterrent to continued aggression or as a compellent means of intimidation, often seems to require interpretation … as an action that enhances the risk of a greater war."* – and in the same way, the purpose of entering the Grey zone at all can be to manipulate risk. (3) A key distinction from ambiguity is that probabilities are better understood with risk, and thus good baseline data can help turn events from ambiguous to risky. (4) Evidence from criminology suggests criminals are only poorly influenced by deterrent threats. One potentially important finding for deterrence at the population level in the Grey Zone is that it the *likelihood* of punishment appears to have more deterrent impact than the *severity* of punishment.

Finally, Chapter 5 discusses "Prospect Theory", "Madman Theory" and Iran's use of Grey Zone tools including risk and ambiguity. For a more detailed discussion of risk and ambiguity in space, including in the Grey Zone, please see Wright (2018) MindSpace: Cognition in Space Operations.

Chapter 6 Legitimacy, fairness, honour and status

This chapter discusses a group of powerful, connected human motivations that are crucial in Grey Zone competition: fairness, legitimacy, honour and status. They are interconnected. What an audience perceives as "fair" or "legitimate" will be powerfully affected by what their "status" makes them perceive they are entitled to. Accepting injustice may be go against ideas of "honour" central to the ethos of warriors and statesmen since Ancient Greece as described by Thucydides. Policymakers can harness these powerful motivations to cause intended and avoid unintended effects. Specifically:

Fairness: Adversaries may pay high costs to reject perceived unfairness, which can lead to deterrence failure or escalation. Fairness takes many forms and this drive should be included when analyzing an audience's decision calculus. It may mean *greater* deterrent threats are required than without anticipating this motivation. Strategies to minimise perceived unfairness may be needed to manage escalation of Grey Zone conflict.

Legitimacy is a source of influence – and should be actively planned for as a source of influence Perceived legitimacy of actions partly determines their impacts on adversaries, allies and other third parties.

Perceived fairness and legitimacy are fundamentally subjective. When making an action, one must ask: *"how fair will this be perceived to be fair and legitimate by key audiences?"*

Status: An audience's understanding of their social status affects what they perceive they are entitled to. Nationalism affects status seeking and entitlement. Status should be used to help motivate individuals within populations, particularly where those individuals' outputs are difficult to measure.

Local groups in a Grey Zone conflict, such as in Ukraine, may be impossible to reconcile unless proposed settlements are perceived to deal with their self-interest, fear and fairness.

Chapter 7: Norms and norm change – the neural phenomenon of "prediction error"

Managing change is key to the international system. Change will always occur, for example from technological, demographic or economic drivers. Failure to manage change can lead to war.

Norms are the "rules of the road" in the international system. Managing potential changes in norms is critical in the Grey Zone – and *in the Grey Zone U.S. policymakers should regard managing potential changes in norms as an end in itself.*

The neural phenomenon of "prediction error" is critical to how humans change their expectations about the world – unexpected events that violate norms change those norms. Thus, the policymakers must manage unexpectedness and unpredictability in the Grey Zone. For instance:

- Breaking a norm can be deliberate, to shock. Soviet leader Nikita Khrushchev banging his shoe on the table in the UN. Chinese leader Deng Xiaoping hugging the prime minister of Japan. Sadam Hussein's use of chemical weapons. Syrian use of chemical weapons.
- Salami slicing and ambiguity can be used to change norms without causing significant prediction error and thus less psychological impact.

Chapter 8 Deterrence and escalation management – both are cases of influence

Grey Zone conflict is necessarily limited – and thus an isolated focus on either deterrence or escalation management alone is insufficient. This chapter outlines a practical framework for influence, which incorporates both deterrence and escalation management. Key points include:

(1) Deterrence and escalation management are intimately related and are both cases of influence. Moreover, neither alone is sufficient for the U.S. to cause intended and avoid unintended effects in the Grey Zone – *and both should be considered together within the framework of influence.* Using only the concept of deterrence, for instance, to design strategy for the ongoing Grey Zone competition with North Korea is incredibly difficult because escalation management *must* also be considered throughout Grey Zone competition. See Wright (2018) for a discussion applying this report's frameworks to North Korea and East Asia.[1]

(2) Both deterrence and escalation management have a fundamentally cognitive dimension. A realistic account of audience decision-making must lie at the heart of any influence strategy – The "checklist for empathy" in Part I of this report provides one simple, operationalisable example, based in evidence.

(3) Culture should be taken seriously to understand the adversary. Understand potential adversaries' concepts of deterrence and escalation management. For example, Chinese deterrence concepts centre on managing a psychological balance and may involve pre-

---

[1] Wright, ND (2018) *Getting Messages Through: The cognition of influence with North Korea and East Asia*, Intelligent Biology. Available from www.nicholasdwright.com.

emption. The U.S. must anticipate such events within the Chinese deterrence paradigm. I discuss how, practically, to get to grips with culture.

(4) Finally, I emphasize three often overlooked factors in escalation management:

- Controlling escalation involves not just minimising escalatory factors, but also positive accommodative and conciliatory gestures.
- Escalation or de-escalation can result from events' predictability and unexpectedness. The U.S can manage this "prediction error."
- Perceived fairness matters in shaping deals and deterrence (see Chapter 6).

<u>Part III Cyber in the Grey Zone</u>

Part III examines cyber in the Grey Zone. Chapter 9 asks if cyber presents particular challenges in the Grey Zone and, if so, what these mean for the U.S.. Chapter 10 looks specifically at Chinese and Russian cyber Grey Zone activities against audiences outside their borders at both the state and population levels.

<u>Chapter 9: Cognitive Factors in Grey Zone Cyber</u>

Cyber activity presents specific challenges in the Grey Zone:

- Technology changes, but the humans on the receiving end of influence remain human. The aim is to influence human psychology, so cognitive factors provide a solid bedrock for anticipating cyber effects.
- New technologies provide opportunities for potential adversaries to leapfrog U.S. cyber capabilities and to pursue highly asymmetric strategies.
- "Chemically pure ambiguity": Difficulty attributing cyber actions magnifies the challenge of ambiguity in cyber. Ambiguity and attribution problems are central to cyber – not only difficulties in Governments establishing unambiguous versions of events (e.g. a DPRK or Russian source of a cyber action that may justify retaliation) but also in communicating that unambiguously to key local and allied audiences.
- Greater difficulty defining the Grey Zone's lower and upper boundaries in cyber-conflict increase the potential for escalation.
- The unexpected nature of cyber activities to those on the receiving end may render them more escalatory than is understood by those making the actions.

This chapter first looks at the characteristics of cyber in the Grey Zone. It then discusses how cyber relates to key factors in the Grey Zone competition identified earlier in the report: ambiguity, fairness and legitimacy, norms, deterrence and escalation management.

<u>Chapter 10: Russian and Chinese cyber approaches</u>

The overwhelming US dominance in conventional warfare forces revisionist states to employ asymmetric means in order to achieve political objectives – and cyber presents such an opportunity. How Russia and China seek to do this is shaped by:

- Russian and Chinese cyber policy appears to emphasize a different set of security challenges to its US and UK counterparts. Both states take a more cognitive and

holistic socio-technical view of cyber- and information warfare and security; than the narrower euroatlantic understanding of the cyber domain.

- Moreover, their domestic information operations significantly shape Russian and Chinese foreign information operations. Indeed, China in 2011 spent more on domestic security than on external security ($111 vs. $107 billion).

This chapter looks specifically at Chinese and Russian cyber Grey Zone activities against audiences outside their borders at both the State and Population levels. Given the importance of their domestic activities, and the difficulty in identifying Russian and Chinese external activities using only information from the public domain, we also describe their domestic cyber security activities.

Part IV Measuring Influence in the Grey Zone

Chapter 11 Measuring the impact of influence

Measuring impact is necessary to understand effectiveness, improve influence activities and ensure accountability. It can be achieved without excessive administrative burden. Key points include:

(1) Planning and resourcing for evaluation is key. This needs to happen both before and after the intervention occurs. Evaluating multiple projects across contexts is necessary to answer key questions on impact, e.g. about contextual factors. Storing cases of success and failure is key for organisational learning.
   - Consider baseline measurements (e.g. polling) ahead of time, as often influence campaigns occur without comparator groups.
   - Government should develop a clearinghouse of validated (and rejected) influence measures. This will give practitioners easy access to a database of measures tried and tested. This presents security challenges.

(2) Rigour is the key concept in measuring impact, it is about being thorough and careful. Rigorous measurement can be qualitative (interviews, focus groups, observation) or quantitative (surveys, experiments).
   - Try to combine methods where possible.

(3) Behaviour change, perceptions or attitudes can all be the focus of measurement. Side effects such as in the target or other audiences, effect size, effect duration and context effects will also be important.
   - Measure behavioural change where possible, as well as attitudes or perception. Try to specify these metrics and side effects before the campaign.

(4) Even if an intervention works, is it worth using? All interventions carry opportunity costs.
(5) Online behaviour presents specific challenges, for example in their relation to offline behaviours.
(6) When facing adaptive adversaries design programs and funding to anticipate counter reforms and multiple battles. Key to this is ensuring flexibility for programmes and budgeting and testing hypotheses throughout a programme's life cycle.

Chapter 1: Introduction

[Strategic thought] 'draws its inspiration from each century, or rather at each moment of history, from the problems which events themselves pose.' - *Raymond Aron*

1.1.   This introduction discusses key concepts for successful Grey Zone strategy:

> ➤ Grey Zone conflict is necessarily *limited* conflict, sitting between "normal" competition between states and what is traditionally thought of as war.
> ➤ Thus, strategy in the Grey Zone is the art of creating influence. The central aim is to *influence* others' decision-making, rather than removing their capacity to choose using brute force in itself.
> ➤ Influence is affecting audiences' decision-making behaviour, attitudes or perceptions. Technology or geography changes, but the humans on the receiving end of influence remain human - so cognitive factors provide a solid bedrock for anticipating effects.
> ➤ While the nature of conflict remains constant, Grey Zone conflict's character requires different *emphases.* These are the *Five Multiples of the Grey Zone*:
> > o Multiple levels (e.g. influencing populations and states).
> > o Multiple domains (e.g. military, information, economic, cyber)
> > o Multiple timeframes (e.g. ongoing processes and short-term crises).
> > o Multiple audiences (e.g. ally and third party perceptions are crucial)
> > o Multiple interpretations (ambiguity is a key feature)

1.2.   This introduction first discusses what the Grey Zone is (and isn't); strategy in the Grey Zone as the art of creating influence; the five multiples of the Grey Zone; and finally briefly describes the following parts of the report.

WHAT IS THE GREY ZONE, AND WHAT ISN'T IT?

1.3.   Grey Zone conflict is necessarily *limited* conflict, sitting between "normal" competition between states and what is traditionally thought of as war. I define Grey Zone activities as a state's use of single or multiple elements of power to achieve security objectives, using activities that exceed the threshold of normal competition, yet fall below the threshold of conventional war.[2]

1.4.   Grey Zone conflict is not new, with examples across centuries and geographic regions. These range from the Cold War in Africa and Asia, to the years of competition between European great powers before World War I and World War II. The fundamental nature of conflict is unchanged in the Grey Zone. However, the Grey Zone deserves attention now because it is a prominent problem we currently

---

[2] This is similar to a recent report in this same DoD effort, which defines "Gray Zone activities are an adversary's purposeful use of single or multiple elements of power to achieve security objectives by way of activities that cloud attribution, and exceed the threshold of ordinary competition, yet apparently fall below the level of large-scale threats to US or allied security interests." Bragg, B. (2016), "Specifying & systematizing how we think about the Gray Zone", NSI.

face. A recent forecast by CENTCOM Commander General Votel, for example, argued that the majority of threats to US security interests in coming years will occur in a 'gray zone', which they defined as *'characterized by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war.'*[3]

1.5.   However, while the fundamental nature of conflict is unchanged, the Grey Zone requires different *emphases.* I summarise these key challenges as the ***'Five Multiples'*** of the Grey Zone (Box 1.2).

1.6.   Before continuing, I note an advantage to using the term 'Grey Zone' rather than, for example, 'conflict short of war' or 'military operations other than war' – namely that Grey Zone is a positive term, not just a lack of something else. It may not be the kind of conflict for which many in the U.S. military have expected or been trained to fight, but it is a key challenge they must actively embrace.

What Grey Zone conflict isn't: peace or war

1.7.   Grey Zone is neither peace nor war. So, what is war? For scholar Colin Grey 'War comprises more or less, but always to some degree, organized violence motivated by political considerations.'[4] Similarly, Mary Kaldor[5] defines war as 'an act of violence involving two or more organized groups framed in political terms.' She goes on to discuss 'A related terminological issue concerns the word 'conflict'. There is a legal difference between 'war' and 'armed conflict', which has to do with whether or not war has been formally declared. Most data sets assume a threshold below which violence cannot be counted as war – say a thousand battle deaths per year, as in the Correlates of War database.'

1.8.   What is peace? Historian Sir Michael Howard notes the two typically described types of peace:[6] 'Hobbes bleakly defined it [peace] as a period when war was neither imminent nor actually being fought, but this definition is hardly comprehensive. At best this is what is usually described as negative peace' 'Positive peace implies a social and political ordering of society that is generally accepted as just.'

1.9.   The Grey Zone may be neither peace nor war, but is a vague concept in that it is one that has borderline cases that neither clearly fall inside or outside it. It is vague but still useful. An analogy is baldness. My father is now a bald man and when younger had a full head of hair. It is difficult to say when precisely he went from the one to the other, but that does not mean the category 'bald' is not a useful category.

---

[3] Votel J.L., Cleveland C.T., Connett C.T., and Irwin W (2016). "Unconventional Warfare in the Gray Zone", *Joint Forces Quarterly*, (8)0 First Quarter p. 101

[4] Gray C.S. (2010), "War-Continuity in Change, and Change in Continuity," *Parameters* 40, no. 2: 5. p. 6

[5] Kaldor M. (2013) "In Defence of New Wars," *Stability: International Journal of Security and Development* 2, no. 1.

[6] Howard M. (2001) "The Invention of Peace: Reflections on War and International Order", Profile Books, London. p. 2

```
                                    Total war
                                  Limited war
                                         WAR
        ──────────────────────────────────────
                  Many smaller   Single/few    GREY
        Crises      actions     large actions   ZONE
        ──────────────────────────────────────
                    "Normal" competition
        Crises    (e.g. economic competition,  PEACE
                         espionage)
```
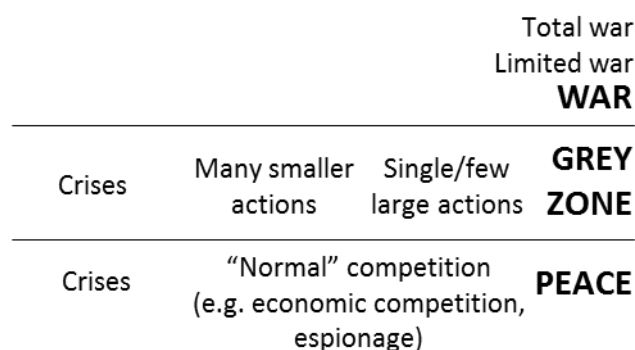
Figure 1.1: Peace, the grey zone and war

BOX 1.1: Changing character and unchanging nature of conflict between humans

A distinction is commonly drawn between the character and nature of war. For instance, Colin Gray[7]: writes that '*Many people confuse the nature of war with its character. The former is universal and eternal and does not alter, whereas the latter is always in flux'* … *'There is only a single general theory of war, because war—past, present, and future—is but a single species of subject. [For example] Air power has made a huge difference to the conduct of warfare, but in a hundred years it has not altered the nature of warfare or war.'*

A key reason human the nature of human conflict remains constant is that it is a strategic interaction between humans, between human psychologies. For example, as Grey further noted: *'The stage sets, the dress, the civilian and military equipment, and some of the language are always changing, but the human, political, and strategic plots, alas, remain all too familiar.'* …'*Interstate war and warfare continue to plague the human race. Even war between great powers is possible, given the political fuel lurking in the twenty-first century in the deadly and familiar classical Thucydidesan categories of 'fear, honor, and interest.''*

STRATEGY IN THE GREY ZONE: THE ART OF CREATING INFLUENCE

1.10. Strategy is fundamentally the same across conflict in many human competitive spheres. Sir Lawrence Freedman's recent book, *Strategy*, illustrates this commonality across three spheres: military, sociopolitical and business strategy. In all three cases: *'The realm of strategy is one of bargaining and persuasion as well as threats and pressure, psychological as well as physical effects, and words as well as deeds. This is why strategy is the central political art. It is about getting more out of a situation than the starting balance of power would suggest. It is the art of creating power.'*[8]

1.11. If strategy is the art of creating power, then what aspect of power matters most in the Grey Zone? Power can be exerted in many ways (Box 1.2) – and given the highly

---

[7] Gray, "War-Continuity in Change, and Change in Continuity." pp. 6-7
[8] Freedman, L. (2013) *Strategy: A History* (Oxford, Oxford University Press).

limited nature of Grey Zone conflict in which audiences are more or less free to choose, influence is the key way to exert power. This is instead of removing their capacity to choose by using brute force in itself. Adversaries can choose whether to act or not (e.g. to be deterred) and whether or not to escalate. Allies can choose whether or not to provide support. Third parties and local populations choose who to who to back and who to oppose.

Box 1.2: Influence and power

I define influence as a means to affect an audience's behaviour, perceptions or attitudes. Influence can be achieved by deterrence, persuasion, 'nudge' or the use of hard or soft power. A key feature of influence is that audiences can choose, which distinguishes influence from the direct effects of brute force that removes the ability to choose. As the late Thomas Schelling wrote in his seminal *Arms and Influence*: 'Military force can sometimes be used to achieve an objective forcibly, without persuasion or intimidation; usually, though—throughout history but particularly now—military potential is used to influence other countries, their government or their people'[9] 'deterrence is about intentions – not just estimating enemy intentions but influencing them.'[10]

Power more broadly consists of the ability to influence choice and removing the capability to choose. Power also contains multiple elements. E.H. Carr's classic work on the Grey Zone between the two world wars—*The 20 Years Crisis 1919-1939*[11]—describes how *'Power is always an essential element of politics.'* Carr then describes three sources of power in international politics: (a) Military Power; (b) Economic Power; and (c) Power over Opinion.

Influence here includes both hard and soft power, which others have previously distinguished between. 'Power is the ability to influence the behavior of others to get a desired outcome. Historically, power has been measured by such criteria as population size and territory, natural resources, economic strength, military force, and social stability'[12] Hard power, is 'the use of military and economic means to influence the behaviour or interests of other political bodies. This is done through the coercion by one political body onto another with a lesser military or economic power.' According to Joseph Nye it is 'Enabling countries to wield carrots and sticks to get what they want.' Soft power, according to Joseph Nye, is 'the ability to shape the preferences of others through appeal and attraction, including through culture, political views and foreign policies.'

FIVE MULTIPLES OF THE GREY ZONE

1.12.   The particular emphases required for Grey Zone conflict is summarized by the ***'Five Multiples'*** of the Grey Zone.

---

[9] Schelling, T.C. (1966) *Arms and Influence* (London: Yale University Press). p. xiv
[10] Ibid. p. 35
[11] Carr E.H. (2001) "The Twenty Years' Crisis, 1919-1939". p. 97
[12] Armitage R.L. and Nye J.S. (2007) CSIS Commission on Smart Power: A Smarter, More Secure America (DC: CSIS).

<u>Box 1.3: Five Multiples of the Grey Zone</u>

➤ Multiple levels
➤ Multiple domains and instruments of power
➤ Multiple timeframes
➤ Multiple audiences
➤ Multiple interpretations

Multiple levels

1.13.   The U.S. must successfully influence multiple societal levels, namely at the *state level* (e.g. adversarial, allied or neutral states); at the *population level* (e.g. mass communication within states and communities); and at the *non-state actor level* (e.g. proxies, violent extremist organisations or quasi-states like Da'esh).

1.14.   We systematically evaluate empirical evidence to identify key cognitive factors for influence at each level. We integrate these into usable tools. For example, a '*Checklist for empathy'* provides a realistic analysis of an adversary, ally and other's decision calculus, which includes key human motivations such as fairness, legitimacy, surprise and self-interest.
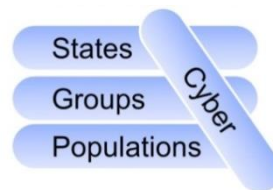
Figure 1.2: Multiple levels and domains

Multiple domains and instruments of power

1.15.   Multiple domains—e.g. military, information, economic and cyber—cut across these multiple societal levels.

1.16.   Key cognitive factors can be common or differ between domains. For instance, managing surprise and predictability (concepts incorporated in a simple *'prediction error' framework* grounded in neuroscience) is critical across domains and levels to cause intended effects and avoid unintended effects.

Multiple timeframes

'There are no endings. If you think so you are deceived as to their nature. They are all beginnings. Here is one.'   *-Hilary Mantel*

1.17.   One must consider at least two separate timeframes: managing an ongoing process evolving over years; and managing short-term crises in light of that ongoing process.

1.18.   Combating propaganda, conducting information operations and messaging more generally at all societal levels critically involves messengers that are trusted and credible to the target audience. Trust is fundamentally psychological, and trusted messengers can often only be created with over longer timeframes (e.g. the BBC).

1.19.   Consider the two biggest historical cases of inadvertent escalation between European powers since 1815: the road to the Crimean War of 1854 in which some 800,000 soldiers died in the Anglo-French versus Russian conflict; and road to the First World War. Both were preceded by lengthy Grey Zone confrontations. U.S. decision-makers must be aware that each episode in the Grey Zone sets the stage for the next interaction. Violating norms, even for admirable reasons, can escalate Grey Zone conflict on a longer timeframe.

Multiple audiences

1.20.   Ally and third party perceptions are critical in the Grey Zone – and U.S. actions will inevitably reach multiple audiences. For instance, if it lost allied support in the South China Sea, the U.S could suffer deterrence by ally denial.

1.21.   Audience analysis is critical across these multiple audiences. This requires both local knowledge within key local audiences, and also the ability of the U.S. analysts to put themselves in the shoes of their audiences – the type of 'outside-in' thinking enabled by our *Checklist for Empathy*.

Multiple interpretations

1.22.   Ambiguity is a key feature of the Grey Zone. Ambiguity's essence is that events or actions are open to multiple interpretations. Ambiguity provides an extra layer of uncertainty even before one consider an event's risk, and can thus directly contribute to crisis escalation. Ambiguity can also help de-escalate crises, for example enabling compromises that save face on both sides (e.g. the 'apology' in the 2001 Sino-U.S. EP-3 incident). In the long run ambiguous actions can change behavioural norms and thus escalate international tensions.

OVERVIEW OF THIS REPORT

1.23.   Part I examines principles for influence in the Grey Zone, making recommendations based on evidence from multiple sources.

1.24.   Part II examines cognitive dimensions of four key aspects of the Grey Zone: risk and ambiguity; fairness, legitimacy and status;

1.25.   Part III examines cognitive factors in cyber within the Grey Zone.

1.26.   Part IV describes how to measure the effectiveness of influence activities in the Grey Zone.

PART I PRINCIPLES OF INFLUENCE IN THE GREY ZONE

Strategy in the Grey Zone is the art of creating influence – but how can we best influence populations and states? Part I provides an evidence-based framework for successful influence. It contains three chapters, each examining how to influence states and populations in Grey Zone conflicts. Chapter 2 describes audience analysis, Chapter 3 describes how to fashion messages, and Chapter 4 describes messengers to deliver those messages.

Methodology of Part I

Part I summarises best practice for influence, based on empirical evidence, for two levels of audience: Populations; and States. It covers aspects of influence relevant to each level, and aspects of influence particularly important to each type of audience. **Footnotes in the text indicate the strength of evidence for each type of audience: Populations; and States.**

Empirical evidence assessed in Part I was drawn from practitioners, academia (including psychology, business, security studies and international relations) and the commercial world; notable recent reports on behaviour change; grey literature produced by non-academic research or practitioner organisations or work cited by policy makers; and searches of academic databases and online resources. Evidence was excluded where it was based solely on theoretical concepts rather than rigorously obtained empirical evidence. Qualitative and qualitative evidence was used where appropriate.

The strength of evidence for key concepts was rated as Strong, Moderate, Low, Nil or Harmful [i.e. counter-productive]. Increased weight was given to convergent evidence (e.g. from diverse disciplines), where it had been shown to matter in the real world (e.g. field studies) and where the methods had been shown to be effective across cultures. Full details of the evidence base for each concept are in Appendix 1.

Chapter 2: Audiences in the Grey Zone

2.1.   Influence efforts must be tailored to the audience to maximise intended effect. Three key messages are:

> ➢ Organisations should adopt an "outside-in" mindset, which makes the audience's decision-making process the focus of the influence strategy. Practical tools can provide the empathy required to put the influencer in the audience's shoes, e.g. to understand their motivations, fears and identities.
> ➢ Messages are likely to reach multiple audiences – it is vital to anticipate potentially divergent influences.

> ➢ Audiences seldom passively receive messages. Audience analysis often requires understanding the ongoing, interactive relationship with messengers.

2.2. This chapter first describes the central importance of thinking "outside-in". It then covers structured approaches to thinking outside-in. The final section is a more detailed discussion of particular factors that influence audience behaviour.

KNOWING YOUR AUDIENCE - THINKING 'OUTSIDE-IN'

2.3. To influence an Afghan farmer not to grow poppy, the influencer must consider that course of action and its alternatives from *the audience's* perspective. If the aim is to deter a hostile State, i.e. influence it not to act, then the influencer must estimate how the hostile State perceives the costs and benefits of acting – and of not acting.[13]

2.4. Embracing an **outside-in** perspective—a mindset that starts with the audience and focuses on creatively delivering something it values—brings benefits relative to an inside-out mindset focused on internal processes that push out products to the audience.[14] In business, this has been a staple of marketing since Harvard Marketing professor Theodore Levitt's 1960 article *Marketing Myopia.*[15] In a more recent study, customer-driven companies doubled the shareholder returns compared to shareholder-driven ones[16] and the advantages are even more marked in the most challenging and turbulent markets.[17] BBC Media Action's development projects in countries such as Afghanistan are critically "audience-centred".[18] In international relations, a key recommendation of Joseph Nye's seminal 2004 book on power and influence is, *"To put it bluntly, to communicate more effectively, Americans need to listen."*[19]

2.5. Influence aims to shape behaviour either immediately or in the future, which requires understanding the audience's decision-making process as shown in Figure 2.1. The decision the audience faces, must be at the heart of planning for influence. Influence is affecting an audience's decision-making process, where that audience can decide between options. The influencer should explicitly estimate that action's perceived costs and benefits and the perceived costs and benefits of alternatives. This includes realistic, conscious and unconscious as well as "irrational" motivations, for example fear, fairness and identity.

---

[13] Freedman, L. (2004) *Deterrence*, 1st edition. Cambridge, UK; Malden, MA: Polity.
[14] **Evidence: Population Strong; State Strong**.
[15] Levitt, T. 'Marketing Myopia', *Harvard Business Review*, July-August, 1960, p.45
[16] Ellsworth, R. (2002) Leading with Purpose, The New Corporate Realities, Stanford Business Books
[17] Gulati, R. (2009) 'Reorganise for resilience: Putting customers at the centre of your organisation', Harvard Business Press
[18] Interviews and www.bbcmediaaction.org [accessed April 2016]
[19] Nye, JS. (2004) Soft Power: The Means to Success in World Politics, Public Affairs, p. 126
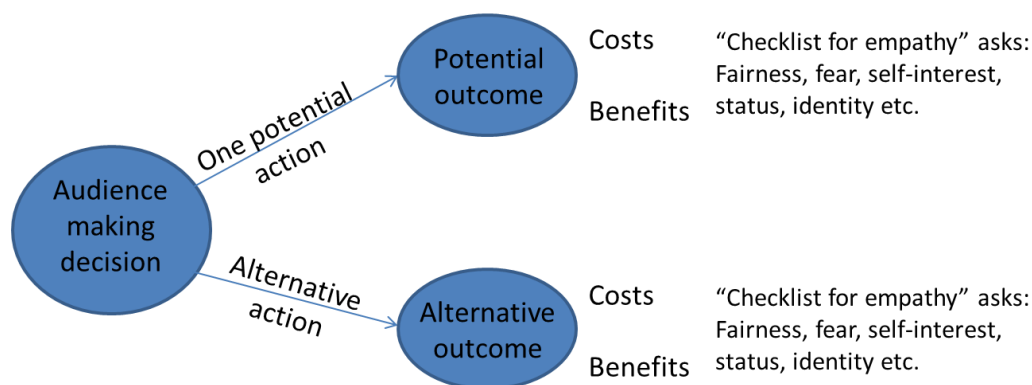
Figure 2.1: The audience decision process.

2.6.   Thinking outside-in seems obvious, yet businesses and governments often fail to do it. One important reason for this is the unavoidable force in any bureaucracy to focus internally on process and known routines.[20] Humans are also predisposed to think egocentrically.[21]

APPROACHES TO THINKING OUTSIDE IN.

A simple approach to thinking outside in

2.7.   Outside-in thinking is very hard. Box 2.1 shows one simple, practical approach to achieving this. Such practical questions as set out in the checklist below can help to estimate the perceived costs and benefits of an action from an audience's perspective – based on a realistic understanding of human motivation and decision-making, coupled with the specific context.

Box 2.1: Checklist for Empathy

A set of practical questions can help to estimate the audience's perceived costs and benefits for their potential alternative actions in a given context, i.e. help complete Figure 2.1. These may include:

  ➢ **Self-interest**: *"What material benefits may they gain or lose?"*[22] The importance of self-interest was shown by the switching allegiances of Sunni groups during the 2007 Surge in Iraq, which involved U.S. rewards and threats of punishment.[23]

---

[20] Allison, G. and Zelikow, P. (1999) *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. Pearson.
[21] Bazerman, M. H. et al (2000) 'Negotiation', *Annual Review of Psychology,* Vol 51, pp279–314, doi:10.1146/annurev.psych.51.1.279.
[22] Paternoster, R. (1995) 'How Much Do We Really Know about Criminal Deterrence?' in *The Journal of Criminal Law and Criminology*, 2010, pp.765–824. Kagel J.H., and Roth, A.E. (1995) *The Handbook of Experimental Economics*, Princeton, NJ.
[23] 'Losing Iraq' (July 29th 2014), Frontline, PBS

> ➢ **Fairness**: *"How fair will it be seen from the audiences' perspectives?"* Humans typically pay costs to reject unfairness and pursue grievances.[24]
> ➢ **Fear**: "Do they fear for their security and why?"[25]
> ➢ **Identity**: *"What are their key identities?"* Humans are driven to form groups ("us", the "in-group") that are contrasted against other groups ("them", the "out-group"). Individuals also often hold multiple overlapping identities.[26]
> ➢ **Status**: *"How may this affect the audience's self-perceived status?"* E.g. For key audiences in Afghanistan, joining the Taliban had high status.[27]
> ➢ **Expectations**: "*What are their key expectations, and what may violate them?"*[28] The more unexpected a perceived event is, the bigger its psychological impact.[29]
> ➢ **Context, opportunity and capability**: *"What opportunities and capabilities does the audience perceive it has for its potential alternative actions?"* E.g. an intervention to encourage someone to pay taxes who is actively avoiding paying taxes, differs to that for someone who feels unable to use an online system.

2.8.   Box 2.2 shows an example of how Hezbollah successfully exploited such audience perceptions. Box 2.2 shows how such motivations help understand an audience, even in a difficult case where the reality for child soldiers is likely to be in stark contrast to that of the influencer.

Box 2.2: Israel losing the information war in the 2006 Lebanon conflict[30]

The July-August 2006 Lebanon conflict with Hezbollah illustrates how an information war can be comprehensively lost over and above the material situation. Amid growing tensions, Hezbollah captured and held two Israeli reservists, leading to Israel Defence Force (IDF) bombardment of both military targets and infrastructure. In turn, Hezbollah launched rockets into Israel and the fighting continued for 34 days with 1,100 Lebanese and 156 Israeli dead. The IDF may have performed well militarily but was widely perceived to have lost the information war among local and global audiences. Why?

---

[24] Camerer, CF. (2003) *Behavioral Game Theory: Experiments in Strategic Interaction*, vol. 9. Princeton University Press, Princeton, NJ.

[25] Posen, BR. (1993) 'The Security Dilemma and Ethnic Conflict' in *Survival*, Vol 35, No 1. pp.27–47, doi:10.1080/00396339308442672; Jervis, R. 'Was the Cold War a Security Dilemma?', *Journal of Cold War Studies* 3, no. 1 (January 2001) pp.36–60, doi:10.1162/15203970151032146.

[26] Sambanis, N., Schulhofer-Wohl, .J, and Shayo, M. (2012) 'Parochialism as a Central Challenge in Counterinsurgency', *Science* 336, no. 6083 pp.805–8, doi:10.1126/science.1222304.

[27] Munoz, A. (2012) *U.S. Military Information Operations in Afghanistan: Effectiveness of Psychological Operations 2001-2010.* Rand Corporation: National Defence Research Institute.

[28] Schelling, T.C. (1966) *Arms and Influence*, Yale University Press; Smoke, R. (1977) *War: Controlling Escalation*, Harvard University Press.

[29] Wright, ND. (2015) 'The Biology of Cooperative Decision-Making: Neurobiology to International Relations', in Galluccio, M (ed.) (2015) *Handbook of International Negotiation*, Springer International Publishing, pp.47–58.

[30] Cordesman, AH. and Sullivan, WD. (2007) 'Lessons of the 2006 Israeli-Hezbollah War*'*, vol. 29, No 4, *Significant Issues Series*, Centre for Strategic and International Studies. The CSIS Press, Washington D.C.

Hezbollah focused on **simple messages** that resonated with key human motivations. This included the perceived **unfairness** of the Israeli response. **Identity** was harnessed against foreign attack by flying Lebanese and Hezbollah flags side-by-side, despite Hezbollah's deep divisions with other groups. In a striking turn around, a poll found 87% of Lebanese supported Hezbollah's resistance, including 80% of the non-Muslim Christians and Druze. Hezbollah rushed aid to damaged areas to minimise backlash from its own supporters. **Expectations** about Israel's military prowess were violated – despite initial success, local audiences perceived the IDF to have been fought to a standstill.

Hezbollah had also invested in **capable messengers**. It skillfully used television and online media to rapidly respond to events. Secretary General Nasrullah was an appealing messenger to key audiences. In contrast, Israel took an **inside-out** approach, largely focused on its own politics, without a realistic understanding of local or international audience responses. It poorly integrated kinetic and information dimensions of its actions.

Structured frameworks for thinking outside in

2.9.   Various other useful tools exist that are based in behavioural and social science, with examples described below that focus on one or more type of audience, e.g. for specific individuals, mass/community communication, organisations/networks and states. Whilst these are based in evidence, there is little direct evidence for the use of the structured frameworks or guides themselves to generate behaviour change, [31] i.e. there is no clear evidence for using one framework in preference to another on the basis of effectiveness. Which is chosen depends in part pragmatically on available time and resources, constraints and aims.

2.10.   There is also limited direct evidence for using a structured framework or guide relative to relative to not using one. However, similarly complex areas for which evidence is available—e.g. use of checklists[32] or structured approaches in health— suggest it is better to use a structured approach (or a blend of approaches) to help prioritise and avoid omissions of key factors. [33] Implementation of such tools suggests local adaptation will likely be important to generate behaviour change within organisations conducting the influence operations.[34]

Structured approaches for different levels of audiences

2.11.   **Specific individuals:** To help understand a specific individual (such as a potential informant or individual undergoing violent radicalisation, their response to disruption

---

[31] **Evidence: Population Strong; State Moderate.**
[32] Gawande, A. (2009) *The Checklist Manifesto: How to Get Things Right*, First Edition. New York: Metropolitan Books.
[33] **Evidence: Population Moderate; State Moderate.**
[34] Anthes, E. (2015) 'Hospital Checklists Are Meant to Save Lives — So Why Do They Often Fail?', *Nature News* 523, no. 7562 p.516, doi:10.1038/523516a.

or diversion; and whether specific messages may resonate) structured tools or frameworks include:

➢ Remote Personality Profiling: Developed by experts in security and psychology,[35] this examines six influences on behaviour: culture and clan; biography and family; personality; the dark side (personality disorders and mental health issues); and motivation. It assesses these using: online and other recorded data (e.g. LinkedIn, biographies, company records of appraisals); human sources (interviews, multi-rater feedback or 360-degree feedback); language and social media.

➢ Structured professional judgement,[36] which draws on psychiatric risk assessment.

➢ Frameworks relating to behaviour change in health, such as the National Institute of Health and Clinical Excellence (NICE) guidelines[37] or "Behaviour Change Wheel"[38] described below (in para. 2.13).

➢ The business and psychology literature contains multiple models for evaluating and influencing others during negotiation.[39]

2.12. **Populations of individuals:** Government may sometimes wish to use mass communication techniques to influence populations of individuals in the public to change their behaviour. For example, to encourage many individuals to improve their internet security. These are not a group or network with connections and relationships but rather a mass of individuals. Much health research on behaviour change works on populations of individuals, as does marketing. BBC Media Action produces media in the developing world, using extensive audience analysis e.g. focus groups, socio-demographics and media analysis.[40]

2.13. One example of a structured approach from health is the "Behaviour Change Wheel", which proposes a 'capability-motivation-opportunity' model for individuals,[41] where capability is further sub-divided into physical and psychological capability, e.g. to think rationally about possibilities; opportunities in the physical environment or social settings; and motivation into reflective (conscious) and automatic (unconscious) processes. In the military information operations sphere, US doctrine specifies a seven step Military Information Support Operation (MISO) process, one stage of which is Target Audience Analysis (TAA).[42] UK doctrine also discusses TAA,[43] with

---

[35] Taylor, J. Furnham, A. and Breeze, J. (2014) *Revealed: Using Remote Personality Profiling to Influence, Negotiate and Motivate*, New York: Palgrave Macmillan.

[36] Author interview with practitioner, February 2016.

[37] National Institute for Health and Care Excellence. Behaviour Change: General Approaches. Available at https://www.nice.org.uk/guidance/ph6 [Accessed 31st March 2016]

[38] Michie, S., van Stralen, MM. and West, R. (2011) 'The Behaviour Change Wheel: A New Method for Characterising and Designing Behaviour Change Interventions' in *Implementation Science,* Vol 6 No 1, p.42.

[39] Malhotra, D. and Bazerman, M. (2012) *Negotiation Genius: How to Overcome Obstacles and Achieve Brilliant Results at the Bargaining Table and Beyond*, Reprint edition, Bantam Books Inc.

[40] Author interview with BBC Media Action, March 2016.

[41] Michie, S., van Stralen, MM., & West, R. (2011) 'The Behaviour Change Wheel: A New Method for Characterising and Designing Behaviour Change Interventions' in *Implementation Science*, Vol 6 No1, p42.

[42] Joint Publication 3-13.2 'Military Information Support Operations', 21 November 2014.

[43] Allied Joint Publication (AJP)-3.10.1 'Allied Joint Doctrine for Psychological Operations', 31 July 2015.

different depths of analysis depending on available resource. There is also a 15 parameter TAA model from the Behavioural Dynamics Institute.[44]

2.14. **Groups, organisations and networks:** for example, deterrence or influence of terrorist groups or cells.[1] Factors to consider here include examining a group's hierarchy, communication methods, the presence of competing subgroups and profiling of the group's leaders. Groups can show "group think", where a desire to conform within a group can lead to overly consensual decisions.[45] Group-level effects may also make groups more extreme than the individuals would otherwise be – a phenomenon known as "group polarisation". Such radicalisation can occur because, in group discussion, each individual hears others' arguments, which, arising from the same mind-set, will also favour risk, with the result that individuals are rationally persuaded by the imbalance of arguments heard in discussion, an imbalance favouring the views most individuals inclined to from the outset.[46] Individuals who move to another place for schooling or work—such as the Hamburg cell of Muslim immigrants involved in the 9/11 attacks—are particularly susceptible to polarization in a new group as they reach out for new ties, a principle used by every army in segregating recruits for basic training. Networks are discussed further in chapter 4. Structured tools for understanding non-state actors overlap with those described below for states such as the use of the Deterrence Operations Joint Operating Concept for non-state actors (para.2.16).[47]

2.15. **At the level of the State** domestic politics is often the key determinant of decision-making.[48] For example, in contemporary Iran, the motivation to reject perceived unfair treatment by outside agents can form an important part of the narrative – when Israel, India and Pakistan have nuclear programs, why can't Iran?[49] Influencing Iran's nuclear behaviour must take account of this motivation.[50] The bureaucratic level matters,[51] for example, competition between different parts of the armed services for limited funding. History also matters deeply to States, for example in China's perceived "Century of Humiliation". As a result, China feels entitled to seek restitution for these past losses, particularly in territorial disputes.[52]

---

[44] Behavioural Dynamics Institute available at www.bdinstitute.org [Accessed 31st March 2016]

[45] Janis, IL. (1972) *Victims of Groupthink*, New York: Houghton Mifflin

[46] McCauley, C. & Moskalenko, S. (2011) *Friction: How Radicalization Happens to Them and Us*. New York: Oxford

[47] Deterrence Operations Joint Operating Concept (2006) US Department of Defense. pp.18-19. Available at http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf [Accessed 31st March 2016]

[48] Putnam, RD. (1988) 'Diplomacy and Domestic Politics: The Logic of Two-Level Games' in *International Organization* Vol 42 No 3, pp.427–60.

[49] Wright, ND. & Sadjapour, K. (2014) 'The Neuroscience Guide to Negotiations with Iran' in *The Atlantic*, 14 January 2014. Available at http://www.theatlantic.com/international/archive/2014/01/the-neuroscience-guide-to-negotiations-with-iran/282963/ [Accessed 31st March 2016]

[50] Einhorn, R. (2014) *Preventing a Nuclear-Armed Iran: Requirements for an Agreement*, Brookings Institution, Washington D.C. available at http://www.brookings.edu/research/papers/2014/03/31-nuclear-armed-iran-einhorn [Accessed 31st March 2016]; Knopf, JW. 'Nuclear Disarmament and Nonproliferation: Examining the Linkage Argument' in *International Security* Vol 37 No 2, Winter 2012, pp.92-132; Albin, C. *Justice and Fairness in International Negotiation* (Cambridge University Press, 2001); Swaine, MD., Zhang, T., and Cohen, DFS., (2006) *Managing Sino-American Crises: Case Studies and Analysis*, Carnegie Endowment for International Peace. See also Chapter 3 in this report.

[51] Allison, G. and Zelikow, P. (1999) *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. Pearson.

[52] Wang, Z. (2012) Never Forget National Humiliation: Historical Memory in Chinese Politics and Foreign Relations. Columbia University Press

2.16.   Structured frameworks at the state level include the US Department of Defense Deterrence Operations Joint Operating Concept (2006)[53] and related analytic tools.[54] In the UK, Dstl is adapting these frameworks.[55] As one analyst describes,[56] the components of a strategic profile include: Historical, ideological and cultural influences; Conditions and belief; Leadership characteristics; Decision-making structures and processes; Strategy and doctrine; and Key uncertainties. An additional approach is the "Red Cell",[57] described in UK military doctrine as a "team responsible for developing an adversary's perspective and Courses of Action (CoAs)".[58]

2.17.   **Hybrid audiences:** Key US conflicts increasingly involve hybrid audiences combining aspects of states and groups. Consider East Ukraine, where one seeks to deter both a highly capable state such as Russia and local groups under their partial control. Daesh contains elements of both quasi-state and groups. This is more complex, and audience analysis here must consider: the motivations of the state; of groups; and the link between the two. For example how much influence does the state have over the groups and in which aspects of their actions?

Dividing up the audience

2.18.   *Within* a target audience, there may be important subgroups with specific decision-making perspectives. Identifying these subgroups can help to identify the relatively small or few audiences whose opinions or actions may cause disproportionate impact. Consider box 2.3 below.

Box 2.3: Selecting an Audience for Political Campaigning[59]

Jim Messina ran Obama's 2012 re-election campaign. The Obama campaign was based on **big data**. The campaigners / analysts combined consumer data, public voting records, responses voters provided directly to campaign canvassers and web cookie data. They spent around $100million on technology, hiring a large staff with mathematical and computational PhDs.

Identify the key audience: All potential swing-state voters were assigned four numbers, each on a scale of 1 to 100:
1 - The likelihood that they would support Obama;

---

[53] Deterrence Operations Joint Operating Concept (2006) US Department of Defense. Available at http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf [Accessed 31st March 2016]
[54] Giles, GF. (2009) 'Waging Deterrence against Iran', pp. 118-9, and Trexel, J. (2009) 'Concepts for Deterrence Operations', pp. 198–9, both in Karl-Heinz Kamp KH. and Yost, DS. (eds), (2009) *NATO and 21st Century Deterrence*, NDC Forum Paper 8. Rome: NATO Defense College Research Division.
[55] Author discussions with practitioners, 2014-2016.
[56] McVicar, M. (2011) 'Profiling Leaders and Analysing Their Motivations', *MORS: Phalanx*, Vol 44 No 4, pp.6-8
[57] Zenko, M. (2015) *Red Team: How to Succeed By Thinking Like the Enemy*, New York: Basic Books.
[58] Ministry of Defence, Development, Concepts and Doctrine Centre 'Red Teaming Guide' 2nd Edition, January 2013. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/142533/20130301_red_teaming_ed2.pdf [Accessed 31st March 2016]
[59] Tufekci, Z. 'Beware the Smart Campaign' *New York Times* (online), November 16 2012. Available at http://www.nytimes.com/2012/11/17/opinion/beware-the-big-data-campaign.html?_r=1 [Accessed 31st March 2016); Beckett, L. Everything We Know (So Far) About Obama's Big Data Tactics in *Propublica* (online), November 29 2012. Available at http://www.propublica.org/article/everything-we-know-so-far-about-obamas-big-data-operation [Accessed 31 March 2016]

> 2 - The likelihood of voting;
> 3 - The odds that an Obama supporter who was an inconsistent voter could be nudged to the polls
> 4 - How persuadable someone was by a conversation on a particular issue.
>
> Critically, this enabled campaigners to focus their resources on the strategic few percent of voters who might switch. So while the Romney campaign knocked on many doors in a street, the Obama campaign could focus on the key one to two houses, with door knockers followed by text messages, etc. They did not assume that voters who said they were "undecided" were necessarily persuadable.

2.19. There are three key methods for grouping an audience:

- ➤ **Audience segmentation** is one method.[60] This categorises a population into different groups, for example using demographic indicators such as age, location or education level. It looks from the audience's perspective at potential self-grouping. This allows the policy maker to target their messaging on the critical audience(s), using the most appropriate message and messenger. As an example, motivation to engage in terrorism for a young woman or man is likely differ and would require different influence approaches to successfully change those motivations.[61]
- ➤ A **'data driven'**[62] approach can sub-divide audiences. This could include using machine learning approaches to cluster individuals into groups, based on available data such as purchase patterns, media consumption or internet meta-data. For instance, Amazon recommendation algorithms[63] rely on homogeneity of interests to recommend additional purchases. Supermarket loyalty schemes profile individuals to personalise offers.[64]
- ➤ **Qualitative approaches.**[65] This includes focus groups, ethnography or unstructured interviews and each can be important to analyse audiences in marketing[66] and for understanding organisational contexts.[67] BBC Media Action's work on programming across the developing world uses these methods extensively.[68]

---

[60] **Evidence: Population Strong; State N/A.**
[61] Jacques, K., & Taylor, P. J. (2008) 'Male and Female Suicide Bombers: Different sexes, Different Reasons?' in *Studies in Conflict and Terrorism,* Vol 31, pp.304-326.
[62] **Evidence: Population Strong; State N/A.**
[63] Mangalindan, JP. 'Amazon's Recommendation Secret' in *Fortune* (online), July 30 2012. Available at http://fortune.com/2012/07/30/amazons-recommendation-secret/ [Accessed 31 March 2016]
[64] Miguéis, V. L., Camanho, A. S., & e Cunha, J. F. (2012). Customer Data Mining for Lifestyle Segmentation. *Expert Systems with Applications*, *39*(10), pp.9359-9366.
[65] **Evidence: Population Strong; State N/A**
[66] Cayla, J. & Arnould, E. (2013). Ethnographic stories for market learning. *Journal of Marketing*, *77*(4), pp.1-16.
[67] Taber, N. (2010). Institutional ethnography, autoethnography, and narrative: An argument for incorporating multiple methodologies. *Qualitative Research*, *10*(1), pp.5-25.
[68] Interview with BBC Media Action staff March 2016.

Key audiences outside the target – intended and unintended

2.20. Identifying key audiences *outside* the target audience is often as critical as looking within the intended target audience. There are two main reasons. First, it can identify key external audiences that serve as the main messengers for the target audience.

2.21. Second, messages are likely to reach multiple audiences whose responses may need to be anticipated. [69] For example, a campaign targeted at youth may also reach their parents. Indeed, the target and additional audiences will likely respond differently to the same message,[70] potentially leading to negative influences outside the target audience.

FACTORS SHAPING AUDIENCE BEHAVIOUR

2.22. A number of different factors can shape audience behaviour and decision making. Understanding these factors aids development of targeted influence approaches.

Identity

2.23. Identity can be a key factor to understand how an audience might respond to influence attempts. "I am a member of the SAS." "I am Pashtun." "I am British." "I am a doctor." This presents both challenges and opportunities, as humans naturally form groups and derive a positive sense of identity from those memberships. Individuals have multiple, overlapping identities. Knowing what kinds of identities are relevant to an individual at any one time will help to understand better how people might make sense of the world, and so how they might act.[71] [72] [73]

2.24. **Identity powerfully shapes audience narratives and decision-making:** Identity provides powerful themes, such as national or ethnic identity, that must be considered in influence campaigns.[74] How identity shapes an audience's decision-making process must also be considered. For example Box 2.4 below highlights how ignoring identity contributed to failed Western influence in Afghanistan.

Box 2.4: Learning from Others, the Taliban

In Afghanistan, the Taliban successfully countered much Western influence, using highly resonant themes of **national identity** and Islam. The Western powers did not harness national identity in Afghanistan, where the Taliban became seen as true jihadists defending Islam and Afghanistan from foreign invaders - highly effective among the Pashtun target audiences. This may have been a missed opportunity, as the Pashtun Wali Shaaker of the US Naval Postgraduate School stated *"they constantly allude to the*

---

69 Evidence: Population Moderate; State Moderate.

70 Bell, A. (1984) 'Language style as Audience Design' in *Language and Society*, Vol 13 No 2, June, pp.145-204

71 Tajfel, H. (1982) 'Social Identity of Intergroup Relations' in *Annual Review of Psychology*, Vol 33, pp.1-39

72 Turner, J. et al. (1987) 'Rediscovering the Social Group: A Self-Categorisation Theory'. Basil Blackwell.

73 Levine, M., Prosser, A., Evans, D.& Reicher, S. (2005). 'Identity and Emergency Intervention: How Social Group Membership and Inclusiveness of Group Boundaries Shapes Helping Behavior' in *Personality and Social Psychology Bulletin*, Vol 31 No 4, pp.443-453.

74 Evidence: Population Strong; State Strong.

> *victorious history of Afghanistan, … but [little] of the literature produced by coalition and U.S. forces appeals to religious and nationalist sentiments of the population in a similar manner."*[75]
>
> National identity or nationalism crucially shapes possible government in such states. There is a need to develop some form of national identity and national narrative that fosters social cohesion and enables the people to defend national interests when necessary but without an anti-"other" centrepiece. This is a missing dimension, albeit for understandable reasons, of much writing on nation- and state-building or counter-insurgency. [76]

2.25. **Multiple overlapping identities:** [77] Individuals have multiple, overlapping identities – for example a Sunni, an Iraqi, a person of a particular clan or profession.[78] [79] Making one of these identities more salient to an individual may influence behaviour.[80] "Social creativity" has been suggested to manage competition over status, whereby different states achieve status in different fields.

2.26. **Inadvertent effects:**[81] Failure to recognise an identity can alienate audiences, for example the impact of security practices in Scottish airports on Scottish Muslims.[82] At airports identity recognition is key, both for the traveler's self-definition and the state's ability to accurately recognise the individual. Some Scottish Muslims reported experiencing airport procedures not as a security and reassurance process but rather as a process of failure to recognise them as legitimate British citizens.

Attitudes

2.27. Attitudes are explicit or implicit evaluative judgements about an abstract or concrete object. Importantly, there is often a big gap between attitudes and actual behaviour,[83] although carefully using attitudinal data can help audience analysis and influence. [84] In particular, attitudes better predict behaviour when they are strong, more

---

[75] Munoz, A. (2012) *U.S. Military Information Operations in Afghanistan: Effectiveness of Psychological Operations 2001-2010.* Rand Corporation: National Defence Research Institute.

[76] Wright ND (2015) *Helping the United States Security Coordinator for Israel and the Palestinian Authority Understand the Minds of Others,* in Wilkenfeld J (Ed.) Strategic Multilayer Assessment White Paper: A Geopolitical and Cognitive Assessment of the Israeli-Palestinian Security Conundrum, US DoD Joint Staff

[77] **Evidence: Population Low; State Low.**

[78] Tajfel, H. 1982, 'Social identity of intergroup relations'. Annual review of Psychology. Volume 33 pp 1-39

[79] Turner, J. et al. 1987, 'Rediscovering the social group: a self-categorisation theory'. Basil Blackwell.

[80] Levine, M., Prosser, A., Evans, D.& Reicher, S. (2005). Identity and Emergency Intervention: How Social Group Membership and Inclusiveness of Group Boundaries Shapes Helping Behavior *Personality and Social Psychology Bulletin*, **31, 4,**, pp.443-453.

[81] **Evidence: Population Low; State N/A.**

[82] Blackwood, L, Hopkins, N & Reicher, S (2015), ''Flying while Muslim': Citizenship and Misrecognition in The Airport' *Journal of Social and Political Psychology*, vol 3, no 2, pp.148-170

[83] Azjen, I. (1991) *'*The Theory of Planned Behaviour' in *Organizational Behaviour and Human Decision Processes,* Vol 50 No 2, pp.179-211.

[84] **Evidence: Population Strong; State Moderate.**

confidently held, less internally inconsistent, less ambivalent and easier to recall.[85] [86] Unformed or ambiguous attitudes are more susceptible to influence.

2.28. Behaviour change can itself change attitudes. [87] As an example, changing energy consumption behaviour leads to continued energy efficient behaviour, even after the initial incentives have been removed.[88]

Age

2.29. As Figure 2.2 shows, despite radically different levels of homicide in England and Wales versus Chicago, the strikingly similar **age** profiles show how young men dominate homicides in both places. This age profile also indicates we may only need to dissuade young men from violence for a few years before their risk is much reduced anyway. Risk-taking is higher amongst adolescents than children and adults, but this depends on context. For example, adolescents take more risks than adults when a peer is with them but not when alone. It also relates to social factors, novelty and sensation-seeking than simply risk.[89] [90]

2.30. Thus, age affects the impact of influence. It is difficult to tease apart how far adolescents and young adults are more directly susceptible to influence than their elders, or whether they are more likely to make high risk decisions in response to influence – but they <u>are</u> at heightened risk of highly negative consequences from malign influence. There is also good evidence that influence has profound impacts on children,[91] hence the key debates globally around school textbooks and mixing of ethnic groups in childhood.

---

[85] Maio, G and Haddock, G. (2010), *The Psychology of Attitudes and Attitude Change*, SAGE publications ltd.
[86] Glasman, LR. & Albarracín A. (2006) 'Forming Attitudes That Predict Future Behavior: A Meta-Analysis of the Attitude-Behaviour Relation' in *Psychological Bulletin,* Vol 132, no. 5, p.778
[87] **Evidence: Population Moderate; State Low.**
[88] Pallak, MS., Cook, DA. and Sullivan, JJ. (2008) 'Commitment and Energy Conservation' in *Policy Studies Review Annual* Vol 4, p.352.
[89] Steinberg, L. (2004) 'Risk Taking in Adolescence: What Changes, and Why?', in *Annals of the New York Academy of Sciences*
[90] Steinberg, L. (2011) 'Adolescent Risk Taking: A Social Neuroscience Perspective', in Amsel, E. & Smetana, J. (eds.) (2011) *Adolescent Vulnerabilities and Opportunities: Developmental and Constructivist Perspectives*, Cambridge University Press
[91] Gass, RH. and John S. Seiter, JS. (2013) *Persuasion: Social Influence and Compliance Gaining*, Fifth edition Boston: Routledge.
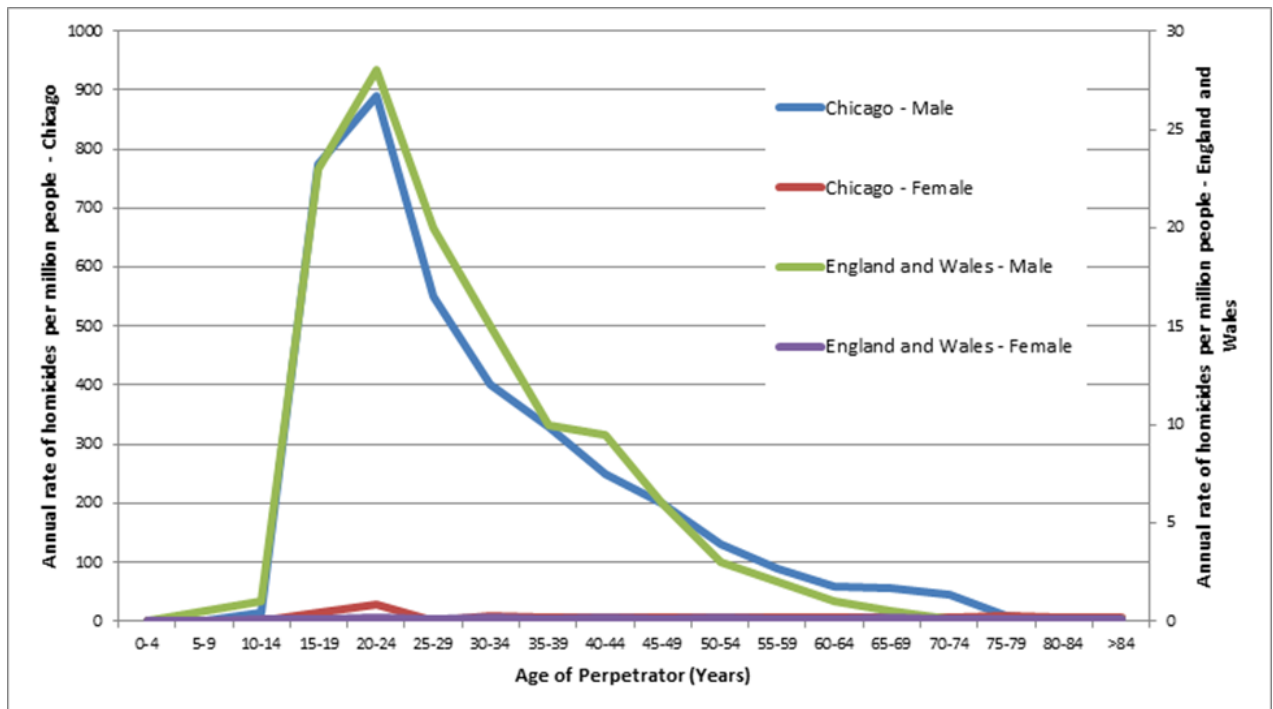
Figure 2.2: Homicides by age and sex of perpetrator, England and Wales compared with Chicago.[92]

Education [93]

2.31.   Limited evidence relates the amount of education to how people respond to information in the West. For example, greater scientific literacy and numeracy in the US led to more extreme views on climate change – and as this occurred for both more individualist and more communitarian individuals, the more educated parts of society became more polarised.[94] Whether type of education affects susceptibility to influence is highly contested, as in disputed suggestions of engineers' susceptibility to violent extremism.[95]

Personality

2.32.   Personality can be characterised according to how a person thinks, feels and behaves, for example by the "Big 5" personality traits.[96] Some measures can be

---

[92] Reproduced from page 132 in Kate Pickett, K. & Wilkinson, R. (2011) *The Spirit Level: Why Greater Equality Makes Societies Stronger*, Reprint edition New York: Bloomsbury Press. Originally from Cronin, H. (1991) *The Ant and the Peacock*, Cambridge: Cambridge University Press

[93] **Evidence: Population Low; State N/A.**

[94] Kahan, DN. et al. (2012) 'The Polarising Impact of Science Literacy and Numeracy on Perceived Climate Change Risks' in *Nature Climate Change*, vol 2, pp.732-735

[95] Gambetta, D. & Hertog , S. (2016) Engineers of Jihad: The Curious Connection between Violent Extremism and Education' Princeton University Press.

[96] Goldberg, L. R. (1990). 'An alternative "description of personality": The Big-Five factor structure' in *Journal of Personality and Social Psychology*, Vol 59, pp.1216–1229.

determined remotely, by social media.[97] Some work suggests personality traits predict receptiveness to influence,[98] for example, that extroverts are less susceptible to influence from authority figures.[99] However, it is unclear how reliable, important and practical such personality measures are for influencing behaviour. [100]

Culture

2.33.   Culture shapes how individuals understand the world and what they value. [101] [102] Well established qualitative methods - interviews, focus groups, ethnography and quantitative methods such as surveys - can capture these effects, so they can be used to design interventions, see box 2.5 below. Contemporary and deeper history also matter. Contemporary reconciliation efforts in Northern Ireland or between States such as China and Japan must consider historical events such as the "Rape of Nanjing" or "Bloody Sunday" that shape narratives and behavioural responses. As with the related issue of identity, cultures are not homogeneous and cultural effects are dynamic and related to context.

Box 2.5: Counter Narrative Operations: Neutralising Al Qaeda in Iraq 2011[103]

During Operation IRAQI FREEDOM, through the summer and autumn of 2010, Al-Qaeda in Iraq led a successful influence campaign on the population of Ninewa province, establishing a shadow government and raising significant financing through taxes and extortion. It recognized that the U.S. was going to withdraw and transition to Operation NEW DAWN but that message, and more importantly the narrative that "the US was transitioning security responsibilities to the competent, well trained Iraqi Security Forces", was not effectively communicated to the population. Al Qaeda in Iraq's competing narrative was that they would defeat the U.S. militarily. It focused improvised explosive device (IED) attacks on routes with high civilian traffic and avoided U.S. combat forces, convoys, and patrol routes. These kinetic actions were conducted in support of Al Qaeda's narrative-focused main effort.

With reduced combat power in Northern Iraq, the U.S. could not effectively launch large-scale kinetic responses. A small team from the U.S applied a mixture of general population polling across the Northern provinces and a method called "cultural domain analysis" to quantitatively measure cultural salience without leading the respondents with structured questions. The results identified that the key cultural goal for residents of

---

[97] Michal Kosinski, David Stillwell, and Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior," *Proceedings of the National Academy of Sciences of the United States of America* 110, no. 15 (April 9, 2013): 5802–5, doi:10.1073/pnas.1218772110.

[98] Hirsh, J. B., Kang, S. K., & Bodenhausen, G. V. (2012). Personalized persuasion tailoring persuasive appeals to recipients' personality traits. *Psychological science*, *23*(6), pp.578-581.

[99] Alkis, N, Taskaya Temizel, T. 2015, 'The impact of individual differences on influence strategies', Personality and Individual Differences, Vol. 87 pp 147-152

[100] **Evidence: Population Low; State N/A.**

[101] Gudykunst, W. B., & Ting-Toomey, S. (1988). *Culture and interpersonal communication.* Newbury Park, CA: Sage.

[102] **Evidence: Population Strong; State Moderate**

[103] Moore et al., 2016 SMA White Paper: Maneuver and Engagement in the Narrative Space, US DoD Joint Staff. Available at http://nsiteam.com/social/wp-content/uploads/2015/12/Maneuver-in-the-Narrative-Space_Final_Jan2016.pdf [Accessed 31 March 2016]

Ninewa was dignity and strength, ideally achieved through courage, generosity and devotion to family.

The results of this are significant. The typical American cultural model is to achieve wealth through hard work and education. Under the American cultural model, a merchant in Mosul that has a successful morning of business and goes home before lunch is lazy, because he is not working hard to make more money. To the Iraqi, however, a merchant who continues to work after a successful morning is greedy, not spending time with his family and denying opportunity to his fellow merchants. Thus, cultural domain provides a window into the driving forces behind behaviour, guilt, motivation and influence. Meanwhile, Al Qaeda in Iraq narratives focused on devotion to Islam, sacrifice and jihad, which did not align with key Iraqi cultural goal. The misalignment of the Al Qaeda in Iraq narrative with cultural values of the population provided an opportunity for manoeuvre and engagement in the narrative space.

The U.S. conducted a series of media programmes ranging from short documentaries, television commercials, to entertainment programmes. Content was optimized to resonate with the population in Mosul, based on cultural domain analysis and general population polling, which included measuring source media outlets relied on for news, information and entertainment. Concepts were pre- and post-tested in focus groups and deployed on appropriate media channels without US attribution. The strategic effects of the programmes were measured again by general population polls to detect statistical deviation from the baseline, as well as through intelligence efforts. The strategic effect of the campaign was a critical information requirement that was tasked to intelligence as part of the intelligence, surveillance and reconnaissance collection plan. The combined results showed a rejection of Al Qaeda in Iraq by the population and financial resources elicited through taxes and extortion fell from $12M per month to a negligible level, where they remained until the rise of Daesh in 2014.

2.34.   The culture of subgroups within societies can be important.[104] Health communication may be improved by segmenting audiences to identify specific groups, tailoring messages and messengers. HIV education aimed at an African-American population was rated more favourably when using a black messenger and tailored messaging, e.g. "Blacks in the United States have always had to stick together just to survive as a people".[105] More individualist or communitarian US political subcultures can markedly differ in their responses to identical information (e.g. about climate change or nanotechnology[106]), leading to increased polarisation – and again this can require using multiple tailored messengers.[107] Within States, the military or strategic community may develop a "strategic culture" or "operational code", which can differ

---

[104] **Evidence: Population Strong; State Moderate.**
[105] Matthew W. Kreuter and Stephanie M. McClure, "The Role of Culture in Health Communication," *Annual Review of Public Health* 25, no. 1 (2004): pp.439–55, doi:10.1146/annurev.publhealth.25.101802.123000.
[106] Dan M. Kahan et al., "Cultural Cognition of the Risks and Benefits of Nanotechnology," *Nature Nanotechnology* 4, no. 2 (February 2009): pp.87–90, doi:10.1038/nnano.2008.341.
[107] Dan Kahan, "Fixing the Communications Failure," *Nature* 463, no. 7279 (January 21, 2010): pp.296–97, doi:10.1038/463296a.

between States, for example leading to potential for misperception and miscommunication between States in crises.[108]

RECOMMENDATIONS

2.35. Ensure an outside-in culture in influence operations, placing the audience's decision-making process at the heart of planning for influence.

2.36. Simple, structured approaches should be used to understand the audience's decision-making process. Practical tools can provide the empathy required to put the influencer in the audience's shoes. Many tools are available; the key is to use a structured approach.

2.37. Influence strategies must anticipate potentially divergent influences, as messages are likely to reach multiple audiences. Audience analysis needs to take into consideration the audience's ongoing, interactive relationship with the messengers. Audiences seldom receive messages passively.

2.38. Identify groups with propensity for influence and who are more likely to act on the basis of the influence they encounter. Their patterns of internet and social media use suggest particular exposure to an array of influential messengers. Focus on these groups and develop specific strategies for influencing them.

---

[108] Snyder, JL. (1977) 'The Soviet Strategic Culture : Implications for Limited Nuclear Operations', RAND Corporation, available at http://www.rand.org/pubs/reports/R2154.html [Accessed 31 March 2016); Katzenstein, PJ. (1996) *The Culture of National Security: Norms and Identity in World Politics,* Columbia University Press.

Chapter 3: Messages in the Grey Zone

3.1. After developing an in depth understanding of the target audience, successful messages must be developed. There are some key concepts that can be applied to development of a successful message.

> ➢ The message must be simple while not leaving an incomplete narrative.
> ➢ The audience must find the message sufficiently credible.
> ➢ Creative implementation of messaging is often key – using novelty and unexpectedness.
> ➢ It must address key audience motivations such as identity, fairness, fear or self-interest.
> ➢ The communication context must be considered – not the message content alone.

3.2. This chapter discusses how to fashion messages, the content of messages and then the context of messages.

FASHIONING MESSAGES

3.3. **Simplicity of message:** Creating a simple message is of prime importance.[109] [110] A simple message that can have personal resonance is most likely to lead to the desired action. Consider Daesh's simple and powerful message to potential Western recruits: Come and belong to our caliphate.[111] To many potential recruits, the Caliphate is a simple, attractive, Utopian vision – and they can belong to it and build it.

3.4. **A complete narrative:** [112] Whilst the headline message must be simple, the influence message should not leave the target audience with an incomplete narrative. People offered incomplete narratives are more likely to revert to previously held beliefs, even those based on misinformation.[113] A complete narrative must offer an alternative explanation and not simply counter the audience's existing view.[114]

---

[109] Cook, J., Lewandowsky, S. (2011), The Debunking Handbook. St. Lucia, Australia: University of Queensland. November 5. ISBN 978-0-646-56812-6. [http://sks.to/debunk]Chip Heath and Dan Heath, *Made to Stick: Why Some Ideas Survive and Others Die*, 1st edition (New York: Random House, 2007).

[110] **Evidence: Individual Moderate; Group Moderate; State N/A.**

[111] Winter, C. (2015) The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf [Accessed 31 March 2016]; Winter, C. (2015) Documenting the Virtual Caliphate, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf [Accessed March 31 2016]

[112] **Evidence: Population Moderate; State N/A.**

[113] Wilkes, A. L.; Leatherbarrow, M. (1988). Editing episodic memory following the identification of error, The Quarterly Journal of Experimental Psychology A: Human Experimental Psychology, 40A, pp. 361-38

[114] Ecker, U. K., Lewandowsky, S., & Tang, D. T. (2011). Explicit warnings reduce but do not eliminate the continued influence of misinformation. Memory & Cognition, 38, pp.1087-1100

3.5. **Credibility:** The target audience should find the message credible enough.[115] [116] For example, deterrent threats—aimed at domestic criminals or foreign states—must include a credible threat of punishment. Mass communication to change public behaviour to counter threats, such as in the 2009/10 Swine Flu Pandemic, requires perception of credible risks.

3.6. **Language and symbols:**[117] It is important to try to use the specific words/terms an audience uses, not those the influencer prefers or is used to.[118] This aids comprehension and increases empathy with the audience. Words with negative connotations for the audience should be avoided and appropriate framing used (e.g. "Death Tax" or "Inheritance Tax").

3.7. **Manage novel approaches:** A novel approach is often more likely to penetrate audiences bombarded by information from multiple sources and who may be jaded, following multiple previous influence campaigns.[119] Daesh continually keeps its executions novel so that they remain salient – for example, using beheadings, then putting those beheadings on-screen (they had been off screen), multiple beheadings, burning to death and using bazookas.[120] Surprise is important in diplomatic and military interactions between States.[121]

3.8. However, unexpectedness should not just be maximised but *managed*. To avoid a large adverse reaction, messages can be gradually introduced over time, to manage the surprise associated with each step. Such "salami slicing" can be effective for individuals[122] and States such as China, e.g. in the South China Sea.[123] [124] Familiarity can increase influence, e.g. increasing rumours' credibility.[125]

3.9. **Organisational structure matters for generating creativity**. Daesh effectively balances a strong coordinating centre with numerous decentralised media units that try different methods to execute that strategy.[126] See box 3.1. Routines also matter – it is important to minimise institutional barriers which may stem creativity. For example, internal approval/clearance processes for influence campaigns must not

---

[115] Gass and Seiter, *Persuasion*.
[116] **Evidence: Population Strong; State Strong.**
[117] **Evidence: Population Strong; State Strong.**
[118] Ibid.
[119] **Evidence: Population Strong; State Strong.**
[120] Winter, C. (2015) The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf [Accessed 31 March 2016]; Winter, C. (2015) Documenting the Virtual Caliphate, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf [Accessed March 31 2016]
[121] Michael I. Handel, *The Diplomacy of Surprise, Hitler, Nixon, Sadat* (Center for International Affairs, Harvard University, 1981); Richard K. Betts and Thomas Mahnken, *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel* (Routledge, 2004).
[122] Cialdini, RB (2008) *Influence: Science and Practice*, 5 edition. Boston: Pearson.
[123] Haddick, R. (2012) Salami-slicing in the South China Sea, Foreign Policy (online) August 3 2012. Available at http://foreignpolicy.com/2012/08/03/salami-slicing-in-the-south-china-sea/ [Accessed 31 March 2016]; Halper, S. (ed.) (2013) China: The Three Warfares. Study for Office of the Secretary of Defense Net Assessement.
[124] **Evidence: Population Strong; State Strong.**
[125] Cialdini, RB (2008) *Influence: Science and Practice*, 5 edition. Boston: Pearson.
[126] Winter, C. (2015) The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf [Accessed 31 March 2016]; Winter, C. (2015) Documenting the Virtual Caliphate, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf [Accessed March 31 2016]

put off the development of creative campaigns in favour of what has been approved before.[127]

3.10. **Oblique messages:** A useful concept in marketing is to present messages obliquely rather than as direct instructions. An example central to BBC Media Action's work in developing countries such as Afghanistan is to use debate programmes on television involving discussion between ethnic and social groups.[128]

Box 3.1: Learning from Others, Daesh

Daesh ruthlessly exploits much of the best practice from across sectors as summarised here. Its products are carefully tailored to its target audiences – as expected if it thought **outside-in** from the audience's perspective. It focuses on key, simple themes in the content of its messages (e.g. victimhood, belonging, Utopianism[129]) very close to the checklist for empathy. Its messages are creative, novel and interesting – to attract the attention of audiences.

Its messengers build up relationships with its audience, through high quantities of messaging. Daesh has also invested in influence capabilities (across social media, local radio and television) and relative to the West can use cheap asymmetric methods. Daesh uses online networks, with key disseminators in the West. Daesh's propaganda structure effectively combines centralisation (e.g. for coordination) and decentralised implementation through multiple competing media units, enabling agility.[130]

CONTENT OF MESSAGES

Tailor messages to the audience

3.11. It is necessary to tailor message content to what is known about the audience. So many permutations exist because context, messenger and audience characteristics each moderate the impact of social influence. Practitioners should assess messages against the types of highly resonant themes identified in Chapter 2, such as in the "checklist for empathy" in Box 2.1, as well as audience-specific factors.

---

[127] Interviews with US Strategic Messaging Practitioners from Departments of State and Defense, October 2015-Jan 2016. [NDW are you happy for me to say this?]

[128] Snow, C. & Taylor, W. (2015) *Media, Discussion and Attitudes in Fragile Contexts*. BBC Media Action Research Report, October 2015.

[129] Winter, C. (2015) The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf [Accessed 31 March 2016]; Winter, C. (2015) Documenting the Virtual Caliphate, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf [Accessed March 31 2016]

[130] Winter, C. (2015) The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf [Accessed 31 March 2016]; Winter, C. (2015) Documenting the Virtual Caliphate, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf [Accessed March 31 2016]

Self-Interest

3.12.   One may seek to use material, monetary or other potential incentives and disincentives to change an audience's perceived costs and benefits of an action and its alternatives. There are many aspects to the use of incentives and disincentives.

3.13.   Incentives have been consistently shown to work in many circumstances:[131] A recent extensive review of deterrent threats on crime[132] shows "offenders and would-be offenders … certainly are rational in the sense that they respond to incentives and disincentives", such as the risk of getting caught and learn as expected after getting away with crime or being punished. However, the effect of deterrent threats is relatively small, and whilst increasing probability of punishments increases deterrence, increasing their severity does not seem to.

3.14.   Positive incentives such as gift giving work well, [133] such as by lobbyists in pharma.[134] States also respond to positive inducements. There are however gain/loss asymmetries,[135] where individuals are more affected by potential losses than potential gains, although how this affects real world decisions is less well understood.

3.15.   Other factors related to incentives which are important to consider include the following:

> *Hassle or transaction costs* can markedly affect many decisions.[136]
> *Incentives' form can enhance effectiveness:*[137] for example by lotteries or surprise.
> *Rebound effects/crowding out:* Using material incentives can crowd out other drivers of behaviour (e.g. moral) so they influence behaviour in the opposite way to that intended.

Fear

3.16.   Fear influences behaviour. For instance in public health campaigns, messengers may attempt to use fear in 'fear appeals'.[138] Fear, for example from terrorism or strategic bombing, causes behaviour change in target audiences.[139] However, this effect typically reduces over time and can be replaced by high resilience and desire

---

[131] **Evidence: Population Strong; State Strong.**
[132] Raymond Paternoster, "How Much Do We Really Know about ppCriminal Deterrence?," *The Journal of Criminal Law and Criminology*, 2010, pp.765–824.
[133] **Evidence: Population Strong; State Moderate.**
[134] Henry Thomas Stelfox et al., "Conflict of Interest in the Debate over Calcium-Channel Antagonists," *New England Journal of Medicine* 338, no. 2 (January 8, 1998): 101–6, doi:10.1056/NEJM199801083380206.
[135] **Evidence: Population Moderate; State Low.**
[136] **Evidence: Population Strong; State N/A.**
[137] **Evidence: Population Strong; State Strong**
[138] **Evidence: Population Moderate; State Strong.**
[139] Bruce Bongar, Lisa M. Brown, and Larry E. Beutler, eds., *Psychology of Terrorism*, 1 edition (Oxford ; New York: Oxford University Press, 2006); Bruce Hoffman, *Inside Terrorism*, 2nd Rev. Ed. edition (New York: Columbia University Press, 2006).

for retribution.[140] Fear is widely accepted as a central driver of inter-State and inter-ethnic conflict as part of the "security dilemma".[141]

3.17. Fear appeal messages are commonly used in influence.[142] Context affects responses to fear appeals and there is debate over whether using fear messages causes positive influence or is counterproductive, e.g. in health campaigns or by doctors advising specific individuals. On balance, fear appeals are likely to be effective,[143] in particular when coupled with credible alternative/preventative behaviours.[144]

Identity

3.18. Identity can provide powerful content.[145] For example, in Afghanistan the Taliban successfully used national identity in its messaging, while this was not stressed by Western campaigns.

Fairness

3.19. Humans are prepared to reject unfairness at substantial cost, and this is rooted in our biology.[146] [147]In a well-known example called 'the ultimatum game', one person gets an amount of money (e.g. £10) and proposes a split with a second person (e.g. £9 for himself, £1 for the other). That other person then decides to either accept the offer, in which case both get the proposed split or reject the offer, in which case both get zero. Even when receiving an offer of free money compared to getting nothing, humans reject offers under 25 percent of the money around half the time.[148] It is not that fairness ought to matter for moral reasons, rather that fairness is important to realistically understand an audience and how it is likely to respond to influence. Examples include:

> ➤ Fairness can help analysts forecast other's decisions more accurately by recognising the costs an audience is prepared to pay to reject perceived unfairness and thus what is needed to compel or deter an action.[149]

---

[140] Bongar, Brown, and Beutler, *Psychology of Terrorism*; Hoffman, *Inside Terrorism*.

[141] Barry R. Posen, "The Security Dilemma and Ethnic Conflict," *Survival* 35, no. 1 (1993): 27–47, doi:10.1080/00396339308442672; Robert Jervis, "Was the Cold War a Security Dilemma?," *Journal of Cold War Studies* 3, no. 1 (January 1, 2001): pp.36–60, doi:10.1162/15203970151032146.

[142] **Evidence: Population Moderate; State N/A**

[143] Melanie B. Tannenbaum et al., "Appealing to Fear: A Meta-Analysis of Fear Appeal Effectiveness and Theories.," *Psychological Bulletin* 141, no. 6 (2015): p.1178.

[144] Melanie B. Tannenbaum et al., "Appealing to Fear: A Meta-Analysis of Fear Appeal Effectiveness and Theories.," *Psychological Bulletin* 141, no. 6 (2015) :p.1178.; Erin K. Maloney, Maria K. Lapinski, and Kim Witte, "Fear Appeals and Persuasion: A Review and Update of the Extended Parallel Process Model," *Social and Personality Psychology Compass* 5, no. 4 (April 1, 2011): 206–19, doi:10.1111/j.1751-9004.2011.00341.x.

[145] **Evidence: Population Strong; State Strong.**

[146] Wright ND. and Schoff J. (2014) *China and Japan's real problem: enter the Fairness Dilemma*, The National Interest. Available at http://nationalinterest.org/feature/china-japans-real-problem-enter-the-fairness-dilemma-11587 [Accessed 31 March 2016]

[147] **Evidence: Population Strong; State Moderate.**

[148] Camerer, *Behavioral Game Theory*.

[149] Albin, *Justice and Fairness in International Negotiation*; Knopf, "Nuclear Disarmament and Nonproliferation"; Nicholas D Wright and Karim Sadjadpour, "The Neuroscience Guide to Negotiations With Iran," *The Atlantic*, January 14, 2014.

- Avoiding perceived unequal treatment of individuals or groups,[150] and stressing equality where possible. For example, framing prevention of radicalisation in young people as safeguarding that is being performed across all in society.
- Procedures should be perceived to be fair – this has been shown to profoundly affect behavioural compliance with US and other police forces.[151] Providing information on procedures and easily accessible justifications of the fairness of the decision-making process.
- Apologies used quickly and appropriately are very powerful. In 2001 a U.S. reconnaissance plane and a Chinese fighter collided, which led to the loss of the Chinese pilot and forced the U.S. plane to land on Hainan in China. The key Chinese demand was for an apology and only when this was perceived to be received was the situation resolved.[152]
- One can highlight perceived unfairness amongst others. For example, noting that in the Islamic State, Foreign Arab fighters earn twice as much as locals, European fighters get three times as much while having few military skills – and questioning whether it is fair that some lives are worth more?[153]

Reciprocity

3.20.   Individuals often feel obliged return a favour.[154] A gift, e.g. a free sample in marketing, can increase response rates.[155] Sequences of offers can be used to create the perception that a concession has been given that leads to "reciprocal" concessions by the audience.[156]

Social norms

3.21.   Norms are any pattern of behaviour common to a group. Norms can scuttle an intervention, and be intentionally used to change behaviour.[157] Simple normative messages provided to households ("99% of your neighbours think that it is a good idea to turn off the lights when you leave the house") have a measurable, long-term impact on energy usage.[158] Even in Rwanda immediately after the genocide, a radio soap opera that presented specific norms of intergroup reconciliation led to cause measurable shifts in intergroup behaviours.[159]. Overall, care is needed: to scrub

---

[150] Stewart, Frances. "Horizontal inequalities as a cause of conflict." Bradford Development Lecture, November. Available at www. brad. ac. uk/acad/bcid/seminar/BDLStewart. pdf. 2009.

[151] Tyler, T.R. (2006) *Why people obey the law.* Princeton: Princeton University Press. and Tyler, T. R. (2011) *Why People Cooperate: The Role of Social Motivations.* Princeton: Princeton University Press.

[152] Swaine, Zhang, and Cohen, *Managing Sino-American Crises*.

[153] (Economist, November 2015).

[154] **Evidence: Population Strong; State Strong.**

[155] Cialdini, RB (2008) *Influence: Science and Practice*, 5 edition. Boston: Pearson.

[156] Cialdini, RB (2008) *Influence: Science and Practice*, 5 edition. Boston: Pearson.

[157] **Evidence: Population Strong; State Strong.**

[158] P Wesley Schultz et al., "The Constructive, Destructive, and Reconstructive Power of Social Norms," *Psychological science* 18, no. 5 (2007).

[159] E.L. Paluck, "Reducing Intergroup Prejudice and Conflict Using the Media: A Field Experiment in Rwanda," *J Pers Soc Psychol* 96, no. 3 (2009).

messages of counter-productive norms (e.g. "60% of young Somali men turn to piracy – help us to prevent this"); and seek norms in line with desired behaviours (e.g. "95% of Somali parents want their children to grow up and have families of their own; help us keep your young men away from a short life in piracy").

Narratives

3.22.   A message may be called a narrative if it is a story that contains information about setting, characters and their motivations. A recent meta-analysis concluded that narratives exert a causal influence on beliefs, attitudes, intentions and behaviours.[160] The size of these effects was similar to other types of persuasive messages and was not found to vary according to medium of presentation. Their broader relevance is illustrated by Lawrence Freedman's extensive historical review of strategic thinking across the military, socio-political and business domains, which placed narrative at the heart of how leaders across these diverse domains often communicate with internal and external audiences.[161]

Coherence of self [162]

3.23.   Individuals prefer to ensure coherence and favourable evaluation of themselves. Thus, having them make a commitment, or having them decide to perform behaviours, may influence them to act in accordance with this self-image in the future. An interesting case is recently discovered Daesh questionnaires for new recruits in Syria[163] who may tick a box for interest in suicide bombing – this small initial commitment may shape later behaviour.

Scarcity[164]

3.24.   Opportunities may be more valuable when they are less available.[165] Individuals tend to value items, opportunities and information more highly when they are less available. However, note that laboratory experiments have shown the reverse in East Asians.[166]

Choice of medium[167]

---

[160] Braddock & Dillard (2016) Meta analytic evidence for the persuasive effect of narratives on beliefs attitudes intentions and behaviors.

[161] Freedman, *Strategy*.

[162] Evidence: Population Strong; State N/A.

[163] http://www.theguardian.com/world/2016/mar/09/isis-document-leak-reportedly-reveals-identities-syria-22000-fighters?CMP=Share_AndroidApp_Gmail

[164] Evidence: Population Moderate; State N/A.

[165] Cialdini, RB (2008) *Influence: Science and Practice*, 5 edition. Boston: Pearson. p200.

[166] Richard Nisbet, *The Geography of Thought: How Asians and Westerners Think Differently...and Why*, 1St Edition edition (New York: Free Press, 2003).

[167] Evidence: Population Moderate; State Moderate.

3.25.   The choice of medium can itself be part of the message.[168] Government has a number of options when it seeks to cause an effect, including: legislation, incentives, traditional media, social media, the use of cultural capital or the use or threat of force. Which is chosen can itself signal, for example, credibility or escalation. In addition, changing between media can be more unexpected and therefore have more impact on audiences.

CONTEXT OF MESSAGES

Contrast and sequences of messages[169]

3.26.   People are tuned to evaluate stimuli by comparing them to other stimuli or options. People were more likely to purchase a cupcake with a free cookie than to purchase a cupcake and cookie in combination for the same price.[170] When such contrasts make the desired behaviour look like the 'better deal', then the influence is more effective. Sequences of messages, particularly in interactions with specific individuals, can generate contrast, e.g.: (1) the "Door in the face" technique described above; (2) "That's-not-all" where a recipient is presented with an initial request, followed by an almost immediate sweetening of the deal, either by reducing the cost or by increasing the benefits of compliance; (3) "Fear-then-relief" where recipients are exposed to an anxiety-provoking message immediately prior to the influence attempt, providing a contrast effect.[171]

Timing[172]

3.27.   Influence can be prepared for on timescales of minutes, e.g. responding to key events on social media, to years (e.g. building institutions such as the BBC or China's Xinhua news agency or global network of cultural Confucius Institutes). When creating a strategy careful thought should be given to the timing of elements and the ability to respond in an appropriate time.

3.28.   Many situations require information within minutes, hours or days. For example, in response to acts of potentially terrorist origin. A slightly different case is during ongoing military campaigns, particularly where there are highly resonant narratives to mitigate.

Standing out against noise

3.29.   The impact of any message is determined partly by the factors set out here and partly by the background volume of all the other information an audience receives.

---

[168] **Evidence: Population Moderate; State Strong.**
[169] **Evidence: Population Strong; State Moderate.**
[170] Berger, J. M. (1986). Increasing compliance by improving the deal: The that's-not-all technique. Journal of Personality and Social Psychology, 51, pp. 277-283.
[171] Cialdini, RB (2008) *Influence: Science and Practice*, 5 edition. Boston: Pearson.
[172] **Evidence: Population Strong; State Moderate.**

'Noise' has been used as a strategy. The Russia Today television network is an interesting example. Rather than promulgating one specific positive explanation of an event, such as the MH17 airliner crash over East Ukraine in 2014, the network created noise by circulating many different (and at times contradictory) explanations. This acted to drown out other messages and create doubt about messages the public did not like, thus creating confusion.[173]

3.30. There is no one clear strategy to stand out against noise. It is likely best achieved by audience-centred approaches that use the techniques above to fashion messages, which are delivered by credible messengers.

3.31. Health campaigns suffer from this challenge. Why should individuals take a new health message seriously when they receive numerous alarming stories and discordant health information?

Counter-messaging against adversaries and competitors

3.32. Counter-messaging can be thought of as intentional and direct efforts to deconstruct, discredit and demystify adversary messaging, whether through ideology, logic, fact or humour. Direct evidence for counter-messaging in a counter-violent extremist context is difficult to obtain and remains limited. However, there is evidence for its utility by analogy with more or less successful news management strategies. This may involve the use of plausible alternative narratives or interpretations of events, for example by analogy with the importance in health campaigns of providing plausible alternative actions for dangerous behaviours.[174]

3.33. In addition, there is evidence for longer-term, broader media strategies to improve community relations. An example is radio soap operas in post-genocide Rwanda (Box 11.3).

RECOMMENDATIONS

3.34. When crafting message content, consider the following

- ➢ Aim to keep the message simple (while not leaving an incomplete narrative), credible, locally adapted and creative.
- ➢ Creativity in messaging is often key – manage novelty and unexpectedness, otherwise messages may lack the salience needed to impact on audiences.
- ➢ Address key audience motivations (e.g. identity and fairness).

3.35. It is vital to consider the communication context – not the message content alone.

3.36. Counter-messaging should be augmented by longer-term, more preventative interventions, e.g. television discussion programmes or radio soap operas involving

---

[173] Cullison, A. (2015) .Malyasia Airlines Flight MH17 Crash Illustrates Different Realities in Russia vs West' in The Wall Street Journal (online) July 22 2015. Available at http://www.wsj.com/articles/mh17-crash-illustrates-different-realities-in-russia-vs-west-1437557400 [Accessed 31 March 2016]; Standish, R. (2015) 'Propaganda Watch: Listen to Two Russians Badly Impersonate CIA Spies to Pin MH17 on US' in Foreign Policy (online), August 12 2015, available at http://foreignpolicy.com/2015/08/12/propaganda-watch-listen-to-two-russians-badly-impersonate-cia-spies-to-pin-mh17-on-u-s/ [Accessed 31 March 2015]

[174] See above for discussion of responses to fear messaging in health.

community cohesion. A coherent media strategy should be part of peri-conflict nation- or state-building efforts.

Chapter 4: Grey Zone Messengers

4.1.   Finding and developing the right messengers is vital. Some key concepts are:

➢ Understanding **networks** can help identify effective messengers.
➢ **Trust** in messengers is often critical. The U.S. or allied Governments are not always the most appropriate messenger. Develop and find trusted messengers.
➢ Messengers must also be **salient** to audiences, they need to stand out to be able to impact psychologically on audiences constantly bombarded by information.
➢ Messengers must be **capable** of reaching audiences.
➢ Key State and non-State actors place influence at the heart of their activities and invest heavily.

4.2.   This chapter examines: messenger characteristics; the importance of networks; the finding and developing trusted messengers; and competition with international actors. Social media and cyber is covered in Part III.

MESSENGER CHARACTERISTICS

Trust and salience

4.3.   Trust is vital when selecting a messenger.[175][176] Perceived trustworthiness or credibility is in the eye of the audience and is highly context dependent. Multiple factors contribute, including perceived expertise, good intentions and capability.

4.4.   **Authority and expertise:** Authority can powerfully influence individuals and the impact of those in official positions or uniform should be considered.[177] Expertise is powerful, even actors playing fictional experts have been shown to wield influence.[178]

4.5.   **Liking and "soft power":**[179] Individuals tend to be more influenced by those they like and be less likely to take advice from those they dislike. Establishing common ground is a means to both influence and relationship building; liking is increased by similarity and similarity increases liking. Self-disclosure by presenting personal information can establish similarity and, independently, increase liking. At the State level, Joseph Nye's original concept of "soft power" was specifically the State's attractiveness to others.[180]

---

[175] Gass, RH. and Seiter, JS. (2013) *Persuasion: Social Influence and Compliance Gaining*, 5th edition. Boston: Routledge.
[176] **Evidence: Population Strong; State Strong.**
[177] **Evidence: Population Strong; State N/A.**
[178] Cialdini, RB (2008) *Influence: Science and Practice*, 5th edition. Boston: Pearson.
[179] **Evidence: Population Strong; State Strong.**
[180] Nye, JS. (2004) *Soft Power: The Means to Success in World Politics*. PublicAffairs

4.6.   **Similarity** of the messenger to an audience increases likely influence.[181] This suggests that minority recruitment in the security services interacting with specific individuals may be beneficial. Messaging to communities or via mass media may benefit from using multiple messengers from different ethnic groups to deliver messages.[182]

4.7.   US or allied Governments are often not the most appropriate messenger. This can be overcome by developing partnerships with trusted individuals and groups. There are often powerful and trusted messengers in areas that Governments and the mainstream media might ignore. For example bloggers of modest fashion, such as headscarves, bring women's voices to wider audiences offline and online – some with several million followers and often based abroad. It is possible to devise interventions to create new messengers. Identifying and developing trusted messengers is discussed below.

4.8.   **Manage messenger salience**: A messenger must be salient—stand out—to gain the audience's attention, consciously or subconsciously. Whilst recognising the factors above, a creative choice of messenger can penetrate audiences constantly bombarded by information. One way to achieve salience is to manage the **unexpectedness of messengers**. Iranian President Rouhani's unexpected use of 2013 Twitter diplomacy changed the political climate and enabled the successful nuclear talks.[183] Repeated exposure to the same messenger can lead audiences to habituate or fatigue. However, **familiarity** with messengers can also increase their influence. Using **multiple messengers** over time enables a campaign to change between them – actively managing unexpectedness helps keep messengers salient.

Capability

4.9.   Messengers must have the **capability** to reach target audiences. **Analysis** helps determine conduits available for influence campaigns. Television, radio and social media impact may vary according to audience. For example, TV may still be most influential amongst key audiences in Iraq.[184] It is no good running a campaign on Twitter if the target audience cannot or does not access it. The BBC World Service is regarded as a reliable and independent news source and yet is less listened to in Russia because it gave up its FM radio frequency.

4.10. **Language** Is a critical factor. A channel may have wide geographical reach but it will be useless if it is not accessible in the language of the intended audience. Often Arabic language channels are presumed to be influential but huge swathes of the Muslim world do not speak Arabic.

IMPORTANCE OF NETWORKS

---

[181] **Evidence: Population Moderate; State N/A.**
[182] Matthew W. Kreuter and Stephanie M. McClure, "The Role of Culture in Health Communication," *Annual Review of Public Health* 25, no. 1 (2004): pp.439–55, doi:10.1146/annurev.publhealth.25.101802.123000.
[183] Wright, ND. & Sadjapour, K. (2014) 'The Neuroscience Guide to Negotiations with Iran' in *The Atlantic*, 14 January 2014. Available at http://www.theatlantic.com/international/archive/2014/01/the-neuroscience-guide-to-negotiations-with-iran/282963/ [Accessed 31st March 2016]
[184] Awad, A. & Eaton, T., (2013) 'The Media of Iraq Ten Years On: The Problems, the Progress, the Prospects'. *Policy Briefing*, *8*. BBC Media Action Page 23

4.11.   Face-to-face, family, social media and other networks can provide key access to audiences. Three issues for the policy maker are:

4.12.   First, what are key social networks amongst the audience? Networks within an audience open specific opportunities for influence, in addition to just broadcasting messages to the network. Trust relationships in networks can drive influence strategies. For example, where a highly trusted node in a network can be identified, they might be recruited or replaced by a friendly messenger and used as a route to influence the wider group.[185]

4.13.   Second, what networks link the audience to the outside? Trust exists in networks, so networks can be good messengers to access an audience.[186] One can also deliberately build up key favourable messengers.

4.14.   Third, who are key **opinion leaders**[187] in these networks on whom activity could be focussed? A recent report by King's College London[188] used a quantitative analysis of the social media profiles of 190 Western and European foreign fighters, of whom over two thirds were affiliated with Jabhat al-Nusrah or Daesh. They report that, based on "their popularity within foreign fighter networks, the paper identifies the two most prominent of these new spiritual authorities as Ahmad Musa Jibril and Musa Cerantonio. Jibril, a U.S. based preacher with Arab roots who is in his early 40s, does not explicitly call to violent jihad but supports individual foreign fighters and justifies the Syrian conflict in highly emotive terms. He is eloquent, charismatic, and – most importantly – fluent in English. So is Musa Cerantonio, an Australian convert to Islam in his early thirties who frequently appears on satellite television and has become an outspoken cheerleader for ISIS. Both men are very different and consequently have different appeals. Ahmad Musa Jibril is a subtle, careful and nuanced preacher, while Musa Cerantonio is much more explicit in his support for the jihadist opposition in Syria."

FINDING AND DEVELOPING TRUSTED MESSENGERS

Finding trusted messengers

4.15.   **Network analysis** can identify formal and informal opinion leaders or networks, for example using qualitative methods in communities (e.g. focus groups) or quantitative social media analysis.

4.16.   The use of **family** members delivering a message can be important.[189] Indeed, the first covert CIA mission used Italian Americans to write letters to Italian relatives to influence the result of the 1948 election.[190] In Afghanistan, Western forces under-

---

[185] **Evidence: Population Moderate; State Moderate.**
[186] **Evidence: Population Strong; State Moderate.**
[187] **Evidence: Population Moderate; State N/A.**
[188] Carter, JA., Maher, S., Neumann, PR. (2014) #Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks, ICSR, King's College London
[189] **Evidence: Population Strong; State Strong.**
[190] Mistry, K. (2011) 'Approaches to Understanding the Inaugural CIA Covert Operation in Italy: Exploding Useful Myths', *Intelligence and National Security* Vol 26, no. 2–3 (April 1, 2011): pp.246–68, doi:10.1080/02684527.2011.559318.

used these techniques in favour of other media, such as newspapers, that were of little use.[191]

4.17.   Daesh makes use of key influencers and supporters who wield considerable influence online.[192] Because they are based mostly in the West, such disseminators have significantly eroded the ability of Daesh to exert central control over information.[193]

Developing trusted messengers

4.18.   *Mass communication to populations:*[194] Developing a trusted organisation, such as the BBC, takes many years. Critically it builds a *relationship* with audiences.

4.19.   In the UK, the latest Ofcom survey of public service broadcasting reports that two in three UK adults rated highly that the delivery of 'Its news programmes are trustworthy'. This covered BBC One, BBC Two, the Channel 3 services, Channel 4 and Channel 5, the BBC portfolio channels and S4C. 70% of those interviewed thought it important that the BBC 'provides a website with high quality content that you can trust', and 90% who have used the BBC website in the last month said they were satisfied.[195]

4.20.   Data on trust in the BBC overseas is harder to collect, although detailed data is available for the United States. In 2014, Pew examined online Americans' trust in 36 news organisations for news about government and politics. 36% trusted the BBC, which ranked 8th after major US networks with CNN topping the poll with 54%. The BBC ranked ahead of the New York Times (34%), Wall Street Journal (37%) and NPR (29%). As the BBC was somewhat less well known than the major US networks--76% known compared to 95% for CNN—Pew thus turned to the ratio of those who trust against distrust the source. Here the BBC ranked 2nd of the 36 news organisations, with 36% trusting, 7% distrusting and 33% neither.[196]

4.21.   *Within local communities* specific individuals can have their status enhanced, to act as influencers within their existing networks. [197] For instance, taking Afghans to Mecca, accompanied by US Special Forces, raised their status when they returned with more favourable opinions of the West (see Box 4.1). An anti-Female Genital

---

[191] Munoz, A. (2012) *U.S. Military Information Operations in Afghanistan: Effectiveness of Psychological Operations 2001-2010.* Rand Corporation: National Defence Research Institute.

[192] Carter, JA., Maher, S., Neumann, PR. (2014) *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*, ICSR, King's College London; Wood, G. (2015) 'What ISIS Really Wants' in *The Atlantic* (online), February 15, 2015. Available at http://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/ [Accessed 01 April 2016]

[193] Carter, JA., Maher, S., Neumann, PR. (2014) #Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks, ICSR, King's College London

[194] **Evidence: Population Strong; State N/A.**

[195] Ofcom PSB Annual Report 2015. Available at http://stakeholders.ofcom.org.uk/binaries/broadcast/reviews-investigations/psb-review/psb2015/PSB_Annual_Report_summary.pdf [Accessed 31 March 2016]

[196] Mitchell, A., Gottfried, J., Kiley, J. & Matsa, KE (2014) *Political Polarisation and Media Habits*. Pew Research Center: Journalism and Media. October 21 2014. http://www.journalism.org/2014/10/21/section-1-media-sources-distinct-favorites-emerge-on-the-left-and-right/#smaller-audience-but-strong-trust [Accessed 31 March 2016]

[197] **Evidence: Population Low; State N/A.**

Mutilation programme in Kenya taught young people cricket, which gave them sufficient status to be heard by their elders about FGM.[198]

Box 4.1: Successful Counter-narrative Operations, Voices of Moderate Islam[199]

Operation "Voices of Moderate Islam" carried out in Afghanistan in 2010 was designed to resonate with existing indigenous narratives. The programme's goal was to counter the adversary's prevailing narrative to degrade their recruiting efforts and de-legitimize their local operations. The prevailing narrative in the provinces was that the Coalition Forces were attempting to supplant Islam with Christianity. The operation was built with this in mind and tailored to the goal of using narrative as a vehicle to counter a critical thread of the Taliban narrative by demonstrating that the U.S. and Coalition Forces were not at war with Islam.

During the operation, soldiers accompanied 33 "Afghan Key Communicators" on an Islamic pilgrimage through Jordan *en route* to Saudi Arabia. These "Key Communicators" were handpicked from the general population to represent a wide swath of Afghan society and included village elders, members of the Afghan National Security Forces, former Taliban fighters and other influential individuals. During the trip, which was planned during the holy month of Ramadan, the Key Communicators performed the rite of Umrah and earned the honorific "Hajji." With this honour bestowed on them, the Afghans readily returned to their home villages and began to disseminate unscripted narratives that painted a different, yet more credible picture than the one the adversary was providing.

For a fraction of the cost of a single aircraft sortie, the United States was able to counter the opposition's prevailing narrative by demonstrating that the Coalition was not attempting to supplant Islam with Christianity, nor was the West at war with Islam. At some point in the operation each participant internalized the intended coalition message that multi-national efforts in Afghanistan did not constitute a "war on Islam." Participants in the programme had their beliefs fundamentally changed. Many of the Afghans had not travelled from their home villages before, much less travelled on an airplane to a foreign nation. The personal narratives the participants would create and tell for the rest of their lives would then challenge the belief system of every member of their society who previously believed that Coalition Forces were against Islam. One participant explained the experience: "I can speak for us all when I say, we never knew that American bases here had mosques on them, or that you had Muslim Soldiers in your Army, that you would allow them to pray and observe Ramadan. I thought you were only about killing – but now I see so much more." Another participant noted: "This journey is our life. When we return, we will tell others what we saw here, we will tell others what you did for us. Everyone will know of the respect you have shown us." Because these men are **credible** within their

---

[198] Ford, L. (2015) 'Masai Cricket Warriors Determined to Hit FGM for Six' in *The Guardian* (online) 12 November 2015. Available at http://www.theguardian.com/global-development/2015/nov/12/maasai-cricket-warriors-female-genital-mutilation-movie-last-man-stands-championship [Accessed 31 March 2016]; http://www.bbc.co.uk/mediacentre/latestnews/2015/combined-global-audience [Accessed 31 March 2016] http://www.bbc.co.uk/ariel/27905733 [Accessed 31 March 2016]

[199] Moore et al., 2016 SMA White Paper: Maneuver and Engagement in the Narrative Space, US DoD Joint Staff. Available at http://nsiteam.com/social/wp-content/uploads/2015/12/Maneuver-in-the-Narrative-Space_Final_Jan2016.pdf [Accessed 31 March 2016].

society, their story is logical; it resonates with the people and gives this narrative power to spread. The words the participants use line up with the deeds the participants performed and they have multiple images documenting their story as the narrative spreads.

COMPETITION WITH OTHER ACTORS

4.22.   Many state and non-state actors place influence at the heart of their activities, invest heavily, stress the importance of influence at the highest political and military levels and are rapidly enhancing their capabilities. The U.S. and its allies have great strengths such as the BBC, but this presents a formidable challenge.

4.23.   We next look at four dimensions of this competition: (1) resources and high-level policy support; (2) timescales; (3) concepts; and (4) agility.

Resources and high-level policy support

4.24.   State competitors such as Russia and China have been building powerful, well-resourced messenger capabilities. Adversaries such as Daesh can use cheap asymmetric strategies, such as social media. To compete with both, UK influence capabilities must have appropriate resources, high-level policy support and cross-government organisational structures that provide strategic level coordination with tactical autonomy, adaptability and responsiveness.

4.25.   **Industrial-scale competitors:** State actors are investing heavily in influence. China is investing $7-10 billion per annum in "overseas publicity work".[200] China is building media networks, developing the Xinhua news agency to compete with Reuters and opening Confucius Institutes worldwide. While the BBC World Service broadcasts in 32 languages on an annual budget of $378 million, Russia Today ran just six language services with an estimated budget of over $300 million in 2014.[201] The highest state levels drive these strategies, shown by Chinese President Hu Jintao's 2011 speech on soft power quoted below and by the strategy of Three Warfares (Psychological Warfare, Media Warfare and Lawfare) being endorsed by the Chinese Communist Party Central Committee and the Central Military Commission in 2003. Russia is investing in and developing "ambiguous warfare" techniques, such as used in East Ukraine, that centre on unattributed forces ("little green men"), psychological warfare and bribery.

4.26.   Russia and China also invest heavily in *internal* influence, much of which would be ethically unacceptable in the U.S. but that gives them large-scale, practically experienced influence forces. Chinese examples include tens of thousands of paid commentators who can post huge numbers of comments on social media in response to unfavourable posts from the public – dubbed the "50-cent party",

---

[200] David Shambaugh, *China Goes Global: The Partial Power* (Oxford University Press, 2013).
[201] Legatum Institute, Propaganda Series, September 2015. *Information at War: From China's Three Warfares to NATO's Narratives*. Available at https://lif.blob.core.windows.net/lif/docs/default-source/publications/information-at-war-from-china-s-three-warfares-to-nato-s-narratives-pdf.pdf?sfvrsn=2 [Accessed 31 March 2016]

because they were reputed to be paid 50 Chinese cents for each positive posting.[202] Harvard's Gary King recently uncovered more sophisticated influence techniques by examining what posts were taken down by Chinese censors: *"Criticisms of the government in social media (even vitriolic ones) are not censored, whereas any attempt to physically move people in ways not sanctioned by the government is censored …even posts that praise the government are censored if they pertain to real-world collective action events."*[203]

4.27. **Asymmetric costs:** Just as Improvised Explosive Devices cost adversaries only a few dollars but imposed huge, asymmetric costs on Coalition forces in Iraq post-2003, so too can adversaries compete with us asymmetrically in the information space. Daesh can produce high quality, fast, highly effective products that impact on target audiences in the region and Western countries.

4.28. **High-level policy support:** State and non-State actors stress the importance of influence and drive this investment at the highest levels. For example:

> ➢ "We should bring Chinese culture to the world, develop cultural soft power compatible with China's international standing and increase the influence of Chinese culture in the world" – Chinese President Hu Jintao, 2011[204]
> ➢ "The very "rules of war" have changed. The role of non-military means of achieving political and strategic goals has grown and, in many cases, they have exceeded the power of force of weapons in their effectiveness." – Gen. Valery Gerasimov, Chief of General Staff of Armed Forces of Russia, 2013
> ➢ "We are in a battle, and more than half of this battle is taking place in the media." – Ayman al-Zawahiri, Current Leader of Al-Qaeda
> ➢ The US Army is radically changing its doctrine to add a "seventh warfighting function" called "engagement", which will involve skills used to influence foreign governments and militaries.

Timescales

4.29. Interacting with capable competitors requires preparing for influence on timescales of **minutes,** such as responding to key events on social media and the 24/7 newsfeed. This requires a rapid response set within a strategic plan. At that other end of the scale, is the establishment of institutions such as the BBC, which take **years** to build.

Concepts

4.30. The western view of information security fundamentally differs from the Russian and Chinese approaches. Giles and Hagestad (2013) describe this: "Thus the Chinese

---

[202] Bristow, M. 'China's Internet Spin Doctors' on *BBC News* (online) 16 December 2008. Available at http://news.bbc.co.uk/1/hi/world/asia-pacific/7783640.stm [Accessed 31 March 2016]

[203] King, G., Pan, J. and Roberts, ME. (2014) 'Reverse-Engineering Censorship in China: Randomized Experimentation and Participant Observation' in *Science*, Vol 345, Issue 6199; King, G., Pan, J. and Roberts, ME. (2013) 'How Censorship in China Allows Government Criticism but Silences Collective Expression' in *American Political Science Review*, Vol 107, Issue 2, pp.326–343 doi: 10.1017/ S0003055413000014

[204] Shambaugh, D. (2013) *China Goes Global: The Partial Power*. Oxford University Press

view "information space" as a domain, or landscape, for communicating with all of the world's population".[205] This chimes with the Russian view of this space including human information processing, in effect cognitive space. This factor is key to understanding the holistic Russian and Chinese approaches to information security as distinct from pure cybersecurity, a fundamental difference from the western approach to the subject."[206]

4.31.   Concepts of deterrence may also differ between states, potentially leading to misperception. A standard Western view of deterrence between states includes nuclear deterrence, focusing on the threat of force (not its use) and seek to completely prevent adversary actions. However, Chinese[207] or Israeli[208] views of deterrence may include offensive actions to reset a psychological balance and do not necessarily aim to merely reduce adversary actions to an acceptable level.

Agility[209]

4.32.   Adopting an **"outside-in"** perspective discussed in Chapter 1, which starts with an audience and focuses on delivering something of value to it, helps builds more flexible business organisations that cope better with challenging and turbulent markets.[210] This is not only because they attend more to the external environment. It is also because they tend to draw on **external partner organisations** where those partners best help meet audience needs, which can help keep businesses flexible. This can be enhanced by using local knowledge and, where possible, through co-design of interventions.

4.33.   Organisational structure matters. Daesh has a balance between a strong coordinating centre (to set strategy and roll out what is successful) and numerous decentralised media units that can try different methods to execute that strategy.[211]

RECOMMENDATIONS

4.34.   Choose messengers carefully. Messenger choice is itself a tool to increase intended effects and reduce unintended ones. Messengers must also be **salient** to audiences and **capable** of reaching audiences.

---

[205] Giles, K. & Hagestad, W. (2013) 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' In *Cyber Conflict (CyCon), 2013 5th International Conference on Cyber Conflict.* NATO CCD COE Publications, Talinn.

[206] Thomas, T. L. (2001) *Information Security Thinking: A Comparison Of U.S., Russian, And Chinese Concepts.* Foreign Military Studies Office. Available at http://fmso.leavenworth.army.mil/documents/infosecu.htm [Accessed 01 April 2016]

[207] Gerson, MS. (2010) *The Sino-Soviet Border Conflict: Deterrence, Escalation and the Threat of Nuclear War in 1969.* CNA. Available at https://www.cna.org/CNA_files/PDF/D0022974.A2.pdf [Accessed 01 April 2016]

[208] Vinson, M. (2014) "An Israeli Approach to Deterring Terrorism," *PRISM Security Studies Journal* 5, no. 3: 61–75. Rid, T. (2012) "Deterrence beyond the State: The Israeli Experience," *Contemporary Security Policy* 33, no. 1: 124–47, https://doi.org/10.1080/13523260.2012.659593.

[209] **Evidence: Population Strong; State Strong.**

[210] Gulati, R. (2009). Reorganize for Resilience: Putting Customers at the Center of Your Business. Boston, Mass: Harvard Business School Press.

[211] Winter, C. (2015) The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf [Accessed 31 March 2016]; Winter, C. (2015) Documenting the Virtual Caliphate, Quilliam Foundation. Available at http://www.quilliamfoundation.org/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf [Accessed March 31 2016].

4.35.   The U.S and its allies must invest in developing trusted messengers, which will often be long-term, e.g. through community engagement, or foreign BBC services.

4.36.   To improve similarity with audiences, increased minority recruitment for roles interacting with audiences of interest may be beneficial. So too may be the use of multiple messengers from different communities.

4.37.   Networks should be explored to identify messengers.

4.38.   Organisational barriers to timely response should be minimised, within and between messengers.

CASE STUDY: DEALING WITH NOISE – LESSONS FROM PUBLIC HEALTH

(Dr DianeDieuliis, National Defence University, Washington DC)

How can messages or particular narratives withstand the problem of "noise"? With the advent of digital technologies and social media, information is increasingly distributed and received in amounts which frequently overload the human ability to absorb. The challenge becomes how to ensure that particular messages are heard and retained over time. Regarding this issue of messaging amidst "noise", the experience of the public health community in communicating during outbreaks may offer a useful case study and critical observations.

Communication during a pandemic is fraught with political overtones and complicated sociocultural perceptions; some may fear they will not get access to drugs, be unfairly quarantined, restricted from travel, etc. There is also a tendency to want to assign blame which can be directed at the messenger.[212] All of these factors should be considered in building a messaging strategy.

Public health messaging to the primary healthcare community is critical to ensuring that healthcare providers are aware and utilizing the most up to date and informative tools in medicine during any emergency event. This target audience is well educated, has access to many forms of communication, and is typically extremely busy – with limited or purposefully scheduled time for receiving information. Further, they can receive information from multiple kinds of sources (local, state, federal, regulatory, academic, or professional societies, among others), as well as in multiple formats (email, electronic health records, letters, etc.)

In this realm, messaging "noise" is referred to as "information chaos" and is defined in multiple dimensions[213]:

- Receiving too much information
- Receiving not enough information
- Experiencing information scatter
- Receiving information that conflict
- Receiving erroneous information

In terms of cognition, the result of "information chaos" is evidenced by impaired situational awareness of the individual, and increased mental workload, and at worst, can be the cause for errors in family medicine. In a study where health care providers' ability to retain information from messages was measured, recall rates were found to be inversely proportional to the mean number of message received per week. *Just one additional local public health message per week resulted in a statistically significant decrease in the recall of the content message.*[214] This study also demonstrated that information chaos was exacerbated by interruption – that is, when attention is diverted while receiving particular messages, the memory of the message is compromised in favor of the interruption.

A separate study of this community examined whether email or SMS messaging was more effective[215]. The e-mail groups in general showed a higher recall rate than did the SMS group,

---

[212] Douglas M. *Risk and blame: essays in cultural theory*. London & New York, NY: Routledge; 1992.

[213] Beasley, et al. Information Chaos in Primary Care: Implications for Physician Performance and Patient Safety *J Am Board Fam Med*. November-December 2011 vol. 24 no. 6 745-751.
http://www.jabfm.org/content/24/6/745.full

[214] Baseman, et al. Public health communications and alert fatigue. *BMC Health Services Research* 2013 **13**:295.

[215] Baseman, et al. A randomized controlled trial of the effectiveness of traditional and mobile public health communications with health care providers. *Disaster Med Public Health Prep*. 2016 Feb; 10(1):98-107.

without regard to sex, provider type, or organization type. Although these findings suggest that SMS content was less likely to be recalled than content delivered through more traditional communication, it was noted that click- rates were higher in the SMS group than in the other groups. *Encouraging the target audience to access additional information provided in SMS hyperlinks may be a useful strategy for improving awareness of time-sensitive public health message content.*

Importantly, public health often errs on the side of pushing information out, without bidirectional capability. Two-way messaging (beyond noting whether hyperlinks are followed or other remote observations) may be of important benefit in gauging the effects of a messaging strategy. In a survey study of this topic[216], both public health agencies and their stakeholders shared similar values/uses and concerns regarding two-way public health messaging - the choice of a specific strategy needs to balance message content (emergency vs. routine communications), delivery capability (one- vs. two-way), and method (SMS, email, etc.)

While email was overall preferred for receiving public health messages, in an emergency or urgent situation, nearly half of respondents wanted <u>both</u> email and SMS to ensure they received critical messages. Each mode has disadvantages which can be compensated by the other. For example, email is ubiquitous, easily forwarded, unconstrained in message length, and easily referenced as needed. However, in an emergency, electricity and Internet connections may go down, making it impossible to access email messages. SMS is limited in message length, difficult to forward, and perceived as transient. However, in an emergency is often more reliable, and offers the potential for facile 2-way check-ins. *These findings suggest that "tiering" of message type and mode of communication may cut down on "noise" during message overload.*

It is important to recognize that "noise" in messaging or narratives is related to message "fatigue". The public is a more diverse audience with different levels of experience and knowledge of the inciting event. When the public receives too many urgent public health warnings, there can be a perception of scaremongering that damages the narrative's intent.[217] There is evidence to suggest that communicating dire risks associated with and outbreak can be effective, i.e. a scary narrative has some traction, but a more important consideration is the audience's perception of the effectiveness the desired behavior requested by the narrative, and whether there is a lack of negative consequences from engaging in it[218] [219]. A possible exception to this whether members of the target audience have personal experience, or knows someone adversely affected by a disease outbreak: it appears that knowing someone who has been affected makes one more likely to engage with messages and adopt protective behavior[220].

Some general conclusions regarding public communications that avoid "noise" and message "fatigue" have been described. A variety of after action analyses of outbreak communications to the

---

[216] Revere, Debra et al. "Exploring Bi-Directional and SMS Messaging for Communications between Public Health Agencies and Their Stakeholders: A Qualitative Study." *BMC Public Health* 15 (2015): 621. *PMC*. Web. 7 Mar. 2017.

[217] Hilton S, Smith E. Public views of the UK media and government reaction to the 2009 swine flu pandemic. BMC Public Health. 2010; 10: 697. PubMed PMID: 21078169. Pubmed Central PMCID: 2998491.

[218] Rubin GJ, Amlôt R, Page L, Wessely S. Public perceptions, anxiety, and behaviour change in relation to the swine flu outbreak: Cross sectional telephone survey. BMJ (Online). 2009; 339(7713):156.

[219] Rubin GJ, Potts HWW, Michie S. The impact of communications about swine flu (influenza A HINIv) on public responses to the outbreak: Results from 36 national telephone surveys in the UK. Health Technology Assessment. 2010;14(34):183-266.

[220] Rubin GJ, Finn Y, Potts HWW, Michie S. Who is sceptical about emerging public health threats? Results from 39 national surveys in the United Kingdom. Public Health In press.

general public have revealed the features of successful messaging strategies, and the pitfalls of ineffective messaging. Several general principles emerge, as noted by the WHO[221]:

- Build trust during non-emergency events;
- Message early during the campaign;[222]
- A trusted person should deliver the message[223];
- Use transparency in messaging;
- Deliver information that could be acted upon.

During H1N1, efforts were made to try to address these principles. In Mexico, for example, authorities used a *single public health spokesperson, and practiced strict adherence to the same message regardless of source* (television, radio, print). They found that *preexisting and trusted collaborative relationships* between public health and health care organizations enabled successful communication during an emergency. They also observed that excessive, conflicting, confusing, or unnecessarily anxiety-provoking messages were less effective[224].

Regarding transparent, actionable messages, the US Department of Health & Human Services developed pandemic influenza communication tools message mapping. "Message maps" are risk communication tools that organize complex information and make it easier to express, distilling information into easily understood messages written at a 6th grade reading level. Messages are presented in 3 short sentences that convey 3 key messages in 27 words. (The approach is based on surveys showing that lead or front-page media and broadcast stories usually convey only three key messages usually in less than 9 seconds for broadcast media or 27 words for print). Each primary message has three supporting messages that can be used when and where appropriate to provide context for the issue being mapped. These message maps are in the public domain[225].

In sum, some of the general findings here can be applicable to crafting narrative and messages for gray zone operations. With regard to audience, consideration of the following may be helpful:

- Level of knowledge of the narrative content;
- Familiarity/experience with issue relevant to narrative (personal experience, or someone they know);
- level of "information chaos" inherent in target audience;
- how much time they may devote to receiving messages;
- What format the audience prefers to receive messages (noting difference
- Whether it is likely the narrative may be interrupted.

---

[221] http://www.who.int/bulletin/volumes/87/8/08-058149/en/
[222] http://www.vox.com/2014/9/4/6103039/Seven-reasons-why-this-ebola-virus-outbreak-epidemic-out-of-control
[223] https://www.cdc.gov/globalhealth/stories/ebola_communication.htm
[224] Stern, AM, and Markel, H. What Mexico Taught the World About Pandemic Influenza Preparedness and Community Mitigation Strategies, *JAMA.* 2009; 302(11):1221-1222.
[225] http://www.calhospitalprepare.org/sites/main/files/file-attachments/pandemic_pre_event_maps.pdf

PART II KEY PSYCHOLOGICAL FACTORS IN THE GREY ZONE

Part II focusses on cognitive dimensions of four key aspects of Grey Zone conflict. Chapter 5 examines risk and ambiguity. Distinguishing risk and ambiguity helps analysts understand and act within the grey zone. Chapter 6 examines the closely bound human motivations related to fairness, legitimacy, status and honour. Humans will pay high costs to reject perceived unfairness and this can lead to deterrence failure. Grey zone actions must be perceived as legitimate enough to key audiences, including allies or local populations. Chapter 7 discusses how international norms change – a fundamental long-term side effect in Grey Zone conflicts that can eventually escalate the conflict to war. Chapter 8 discusses cognitive aspects of deterrence and escalation management in the Grey Zone.

Chapter 5: Risk, Ambiguity and mastering uncertainty

5.1.   Uncertainty is a strategic challenge in all environments – but it is a particular emphasis in Grey Zone competition. Uncertainty pervades Grey Zone competitions for those making actions, those receiving them and observing third parties. This chapter examines:

> ➢ Uncertainty can be usefully broken down into multiple distinct components that require different policies, in particular risk and ambiguity.
> ➢ Uncertainty in one's judgements—or confidence—is another component of uncertainty and can be crucial for forecasting.
> ➢ "Prospect Theory" and "Madman Theory."
> ➢ Iran's use of Grey Zone tools including risk and ambiguity.

5.2.   This chapter examines each area in turn. For a more detailed discussion of risk and ambiguity in space, including in the Grey Zone, please see Wright (2018) MindSpace: Cognition in Space Operations.[226]

RISK AND AMBIGUITY

5.3.   Risk and ambiguity are central to activities in the Grey Zone. Policymakers can manipulate risk, and use it as a tool for deterrence or escalation management. They can also manipulate ambiguity. Understanding risk and ambiguity is therefore key to achieve intended and avoid unintended effects.

---

[226] Available at www.nicholasdwright.com

*Figure 5.1: Uncertainty can be broken down into risk and ambiguity – which undergo distinct processing in the brain, and which require distinct policy recommendations. **Risk** can be thought of as known uncertainty, for instance betting on the outcome of a coin toss (top left). Risk is shown in the left panel, where you are asked the play a lottery by picking a ball from a bag with 22 balls of which half are black and half white. Thus, the winning chance for each colour is 50%. **Ambiguity** is shown in the right panel. A second bag has the same number of balls, but how many are black and white balls is unknown (shown as grey balls). Adding this extra layer of uncertainty not only leads people to reverse their choices (the famous Ellsberg paradox[227]) but this ambiguity also involves distinct brain processes.[228] Ambiguity is also illustrated by the ambiguous figure on the right panel – is it an old lady or a young lady?*

What are risk and ambiguity?

5.4.   Defining risk and ambiguity are highly contentious because there are multiple overlapping definitions across different disciplines. This is a classic case of different languages in different disciplines (and in normal language) that can't be resolved here. However, the basic concepts are not that complicated or confusing. Risk refers to a situation in which all of the probabilities are known; whilst ambiguity refers to a situation with an extra layer of uncertainty, for instance where some probabilities are unknown.[229]

Ambiguity in international confrontations

---

[227] Daniel Ellsberg, "Risk, Ambiguity, and the Savage Axioms," *The Quarterly Journal of Economics* 75, no. 4 (November 1, 1961): 643–69, https://doi.org/10.2307/1884324.

[228] Dominik R. Bach and Raymond J. Dolan, "Knowing How Much You Don't Know: A Neural Organization of Uncertainty Estimates," *Nature Reviews Neuroscience* 13, no. 8 (August 1, 2012): 572–86, https://doi.org/10.1038/nrn3289.

[229] Antonio Rangel, Colin Camerer, and P.R Montague, "A Framework for Studying the Neurobiology of Value-Based Decision Making," *Nature Reviews Neuroscience* 9, no. 7 (2008): pp.545–56.

5.5.   Ambiguity in events and actions gives an extra layer of uncertainty, so they are open to *multiple interpretations* before we even consider their risk. An analogy is perceptual ambiguity – does the picture in Fig. 5.1 show an old lady or a young lady?

5.6.   Cases include: (1) Ambiguity is a key tool in diplomacy. E.g. the 2001 Sino-US crisis where an EP-3 reconnaissance plane force-landed on Hainan Island was resolved by a letter that could be interpreted one way by the Chinese for their public, another by the US for their public. (2) Russian use of "little green men" makes an offensive action more ambiguous and so more easily deniable – e.g. at least for observing populations in key allies even if not for US security analysts. Countering that ambiguity requires US and allied investment in good communication and attribution capabilities ahead of time, which are trusted by key audiences. (3) How far is a specific action of a local proxy directed by their patron, the adversary? (5) Ambiguous thresholds for deterrent threats enable less loss of face if they are crossed, e.g. compared to hard "red lines". (6) Concessions are critical to managing escalation, and essential when dealing with a nuclear-armed adversary. Ambiguity means they can be offered deniably, e.g. Nixon and Mao initially made deniable overtures to one another before the opening with China. Indeed, clarity too early can prevent later compromise. (7) Economic actions by possible proxies carry ambiguity, e.g. are Chinese companies' investments on key Pacific Islands part of Chinese economic statecraft?

5.7.   Robert Jervis (1970) includes an excellent chapter on ambiguity, particularly in diplomacy.[230]

Risk in international confrontations

5.8.   Risk arises when potential outcomes are uncertain, and this pervades all human decision-making. (1) Consider US, UK and German troops currently deploying to NATO's east, such as the Baltic Republics. Their placement is unambiguous, and provides a tripwire so that there is the risk of escalation if there were serious aggression. This is a classic use of the risk of escalation, as described by Thomas Schelling who devotes a chapter to the "Manipulation of Risk "in his seminal Arms and Influence (1966)[231]. Schelling describes how the risk is that escalation can develop its own momentum and this must be managed, e.g. as during the Cuban Missile Crisis. (2) Schelling also argues that "limited war, as a deterrent to continued aggression or as a compellent means of intimidation, often seems to require interpretation … as an action that enhances the risk of a greater war." – and in the same way, the purpose of entering the gray zone at all can be to manipulate risk. (3) A key distinction from ambiguity is that probabilities are better understood with risk, and thus good baseline data can help turn events from ambiguous to risky.

5.9.   At the population level, we can also draw on extensive empirical literatures from the criminology, public health and terrorism literatures. A wealth of data exists at this population level, for instance as many criminal acts occur across numerous contexts. A recent extensive review of deterrent threats on crime[232] shows "offenders and

---

[230] Robert Jervis, *The Logic of Images in International Relations* (Princeton University Press, 1970).
[231] Thomas C. Schelling, *Arms and Influence* (Yale University Press, 1966).
[232] Raymond Paternoster, "How Much Do We Really Know about Criminal Deterrence?," *The Journal of Criminal Law and Criminology*, 2010, pp.765–824.

would-be offenders … certainly are rational in the sense that they respond to incentives and disincentives", such as the risk of getting caught and learn as expected after getting away with crime or being punished. However, the effect of deterrent threats is relatively small. Moreover, another important finding is that the likelihood of punishment appears to have more impact than the severity of punishment – a finding with applications for Grey Zone activities at the population level.

CONFIDENCE: UNCERTAINTY ABOUT JUDGEMENTS

5.10.   A further aspect of uncertainty is confidence in one's judgements. Friedman and Zeckhauser define confidence or analytical confidence as "the degree to which an analyst believes that he or she possesses a sound basis for assessing uncertainty."[233] The US National Intelligence Council states[234]: "Our assessments and estimates are supported by information that varies in scope, quality and sourcing. Consequently, we ascribe "high," "moderate," or "low" levels of confidence to our assessments as follows:

> ➢ "High confidence generally indicates our judgments are based on high-quality information and/or the nature of the issue makes it possible to render a solid judgment."
> ➢ "Moderate confidence generally means the information is interpreted in various ways, we have alternative views, or the information is credible and plausible but not corroborated sufficiently to warrant a higher level of confidence."
> ➢ "Low confidence generally means the information is scant, questionable, or very fragmented and it is difficult to make solid analytic inferences, or we have significant concerns or problems with the sources."

5.11.   Analysts' estimates of confidence can be important for decision-makers to weigh the advice given by those analysts. Moreover, they can be very useful for the analysts to learn and improve their judgment over time, as shown by Philip Tetlock's extensive research for Intelligence Advanced Research Projects Agency (IARPA).[235] Indeed, confidence estimates play an important role in assessing forecasters and making good forecasts in Tetlock's "Superforecasting" programme. Tetlock's research suggests that "what matters most is *how* the forecaster thinks"[236] – and as Box 5.1 outlines appropriate confidence is one key quality for good forecasting.

5.12.   A potential disadvantage of expressing confidence estimates is spurious exactness. However, as concluded by one recent discussion and literature review on the

---

[233] Jeffrey Friedman and Richard Zeckhauser, "Analytic Confidence in High-Stakes Decision Making: Theoretical Principles and Experimental Evidence from National Security Professionals," (in Press). p. 5

[234] Quoted in Katherine Pherson and Randolph Pherson, *Critical Thinking for Strategic Intelligence*, Second (Thousand Oaks, US: SAGE Publications Inc, 2017).

[235] Philip Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (Random House Books, 2015).

[236] Ibid. p.20

handling of confidence during in the search for Osama Bin Laden[237]: "This article showed that, even if analysts do not state a point estimate, they cannot avoid at least implying one; therefore, they might as well present a point estimate explicitly so as to avoid unnecessary confusion."[238]

Box 5.1: Tetlock and Gardner (2015)[239] "Ten Commandments for Aspiring Superforecasters"

➢ 1) "Triage." "Focus on questions where your hard work is likely to pay off."
➢ 2) "Break seemingly intractable problems into sub-problems." "Decompose the problem into its knowable and unknowable parts"
➢ 3) "Strike the right balance between inside and outside views." "Superforecasters are in the habit of posing the outside-view question: How often do things of this sort happen in situations of this sort?"
➢ 4) "Strike the right balance between under- and overreacting to evidence." "Skillful updating requires teasing subtle signals from noisy news flows"
➢ 5) "Look for the clashing casual forces at work in each problem." "Synthesis is an art that requires reconciling irreducibly subjective judgements."
➢ 6) "Strive to distinguish as many degrees of doubt as the problem permits but no more." "Your uncertainty dial needs more than three settings. The more degrees of uncertainty, the better."
➢ 7) "Strike the right balance between under- and overconfidence, between prudence and decisiveness." "Long-term accuracy requires getting good scores on both calibration and resolution."
➢ 8) "Look for the errors behind your mistakes but beware of rearview-mirror hindsight biases." "Conduct postmortems on failures and successes."
➢ 9) "Bring out the best in others and let others bring out the best in you." "Master the fine arts of team management, especially perspective taking, precision questioning, and constructive confrontation."
➢ 10) "Master the error-balancing bicycle." "Learning requires doing, with good feedback that leaves no ambiguity about whether you are succeeding"
➢ 11) "Don't treat commandments as commandments." "Guidelines are the best we can do in a world where nothing is certain or exactly repeatable."

RISK ACTS DIFFERENTLY FOR GAINS AND LOSSES

---

[237] Jeffrey Friedman and Richard Zeckhauser, "Handling and Mishandling Estimative Probability Likelihood Confidence and the Search for Bin Laden," *Intelligence and National Security* 30, no. 1 (2015): 77–99.
[238] Ibid. p.94
[239] Philip Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (Random House Books, 2015). pp.277-85

5.13. Good evidence exists that risk acts differently when individuals make decisions about gains versus losses. This is seen in the brain and lab behavior[240], as well as in some aspects of influence campaigns as described in Chapter 2 and Appendix 1.

5.14. Importantly, however, given the popularity of "Prospect Theory" amongst many commentators, this is not the same as saying that "Prospect Theory" is correct. "Prospect Theory" is a complicated set of ideas[241] in which just one part is the idea that risk acts differently for gains and losses. Indeed, at the State level in particular it has been particularly difficult to support Prospect Theory, which is largely due to the difficulties of determining baselines for gains versus losses. Prospect Theory is just one theory of choice (and not the first) that involves different effects for gains and losses. New ways to apply the extensive knowledge about how gains and losses affect decision-making to security are currently being developed, grounded in biology rather than one particular academic theory.[242]

"MADMAN THEORY": REPUTATIONS FOR UNPREDICTABILITY

5.15. Manipulating uncertainty about one's reputation, in particular where one is more unpredictable, has been labelled "Madman theory". More research is needed to assess this strategy's effectiveness, particularly at the State level. Sagan and Suri, for instance[243], analyzed U.S.-Soviet nuclear signaling events of October 1969, in which President Richard Nixon may be argued to have pursued such a policy of portraying himself as a "madman." Their conclusion, however, was that: "The existing evidence that the Soviet leadership did not react in any meaningful way to this significant increase of U.S. military readiness suggests that it was also a cheap signal, one that was indicative of a bluff, rather than resolve." [244] Further work is needed.

CASE: IRANIAN MANAGEMENT OF RISK AND AMBIGUITY

5.16. Whilst Iran's strategic culture is relatively poorly understood, the limited work suggests use of ambiguity and multiple instruments of national power – i.e. tools of the Grey Zone.

5.17. Michael Eisenstadt[245] describes the centrality of ambiguity or **multiple interpretations**. "Nothing in Iran is black and white; ambiguity and shades of grey rule. This is both a defining characteristic of Iranian culture, and a reflection of the

---

[240] Wright, N. D., Symmonds, M., Hodgson, K., Fitzgerald, T. H. B., Crawford, B., & Dolan, R. J. (2012). Approach–Avoidance Processes Contribute to Dissociable Impacts of Risk and Loss on Choice. *The Journal of Neuroscience*, *32*(20), 7009–7020

[241] Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, 263–291.; Tversky, A., & Kahneman, D. (1991). Loss Aversion in Riskless Choice: A Reference-Dependent Model. *The Quarterly Journal of Economics*, *106*(4), 1039–1061.

[242] Wright ND (2015) *Neurobiological and Emotional Influences: a realistic organic account of human decision making,* in Wright ND and Astorino-Courtois A (Eds.) Strategic Multilayer Assessment White Paper: The Science of Decision Making across the Span of Human Activity, US DoD Joint Staff

[243] Sagan Scott D. and Suri Jeremy, "The Madman Nuclear Alert: Secrecy, Signaling, and Safety in October 1969," *International Security* 27, no. 4 (Spring 2003): pp.150–83.

[244] Ibid. p.179

[245] Michael Eisenstadt, *The Strategic Culture of the Islamic Republic of Iran: Religion, Expediency, and Soft Power in an Era of Disruptive Change*, 2015. Quotes from pp. 3, 3, 11, 8

fact that ambiguity is often used by the regime as a stratagem to confound its enemies." "Iranian politics are characterized by numerous contradictions and paradoxes. Do not seek consistency where none exists." "Iran has frequently used ambiguity to bolster deterrence. Thus, since 2006, Iranian officials have repeatedly declared that Iran is a "nuclear power," using this term in a way that plays on its multiple meanings."

5.18.   In addition to ambiguity, Eisenstadt also describes the use of **multiple instruments** of national power. He argues that Iran's "Deterrent Triad" rests on: (1) Undertaking subversion and terror on several continents, using proxy and unconventional warfare forces; (2) Economic measures, in particular threatening the flow of oil through the Strait of Hormuz; and (3) Launching long range strikes, primarily by missiles (including against Israel by its proxies and partners, like Hizballah and Hamas).[246]

5.19.   Anthony Cain's earlier analysis of Iran's strategic culture and weapons of mass destruction also stressed that Iran's strategy used **multiple levels**: "The Iranians appear to prefer to act covertly through surrogates to advance their Islamist agenda abroad while simultaneously preserving the territorial integrity of the Iranian state by adopting a strategic defensive posture." [247]

5.20.   Cain also cautions against seeing Iran as a madman type of actor. He writes that "The hypothesis that describes the Iranian strategic culture as more akin to a rational state actor rather than as an irrational and unpredictable religiously fanatic state appears valid."[248] "Ill-considered diplomatic initiatives based upon general perceptions of Iran as an "irrational and unpredictable" actor could reinforce conservative power at the expense of emerging moderate trends. This type of mistake could encourage Iran's predilection toward WMD proliferation while simultaneously making their use more likely."

RECOMMENDATIONS

5.21.   Assess the risks of acting and not acting from the adversary's perspective.

5.22.   Ambiguity is central to the Grey Zone – use it as a tool to minimize the impact of events on key audiences. Countering an adversary's use of ambiguity is difficult and requires sustained information operations to highlight the nature of their activities.

5.23.   Evidence from criminology suggests criminals are only poorly influenced by deterrent threats. One potentially important finding for deterrence at the population level in the Grey Zone is that it the *likelihood* of punishment appears to have more deterrent impact than the *severity* of punishment.

---

[246] Ibid. p. 8
[247] Anthony Cain, "Iran's Strategic Culture and Weapons of Mass Destruction. Implications for US Policy," *Air War College Maxwell Papers* Paper number 26 (2002). p. 17
[248] Ibid. quotes from pp. 16 and 18

Chapter 6: Legitimacy, Fairness, Honour and Status

6.1.   This chapter discusses a group of powerful, connected human motivations that are crucial in Grey Zone competition: fairness, legitimacy, honour and status. They are interconnected. What an audience perceives as "fair" or "legitimate" will be powerfully affected by what their "status" makes them perceive they are entitled to. Accepting injustice may be go against ideas of "honour" central to the ethos of warriors and statesmen since Ancient Greece as described by Thucydides. Policymakers can harness these powerful motivations to cause intended and avoid unintended effects. Specifically:

   ➢ Adversaries may pay high costs to reject perceived unfairness, which can lead to deterrence failure or escalation.
   ➢ Perceived legitimacy of actions partly determines their impacts on adversaries, allies and other third parties. Legitimacy is a source of influence.
   ➢ Perceived fairness and legitimacy are fundamentally subjective. When making an action, one must ask: *"how fair will this be perceived to be fair and legitimate by key audiences?"*
   ➢ An audience's understanding of their social status affects what they perceive they are entitled to. Nationalism affects status seeking and entitlement.
   ➢ Local groups within a Grey Zone conflict, such as in Ukraine, may be impossible to reconcile unless proposed settlements are perceived to deal with their self-interest, fear and fairness.

6.2.   This chapter discusses this constellation of human motivations in the following order: fairness, legitimacy, honour and status.

PERCEIVED FAIRNESS IN THE GREY ZONE

6.3.   Key audiences must perceive Grey Zone actions as sufficiently fair, or sufficiently just. Consider the example of recent Sino-Japanese relations. Grey Zone interactions have been prominent between Japan and China since relations deteriorated steadily around 2012, when their disagreement over who owns some small islands in the East China Sea moved to the front of their bilateral agenda.[249] China made nearly 200 incursions into territorial waters around the disputed Senkaku/Diaoyu islands in 2013, compared to two in 2011 and none in 2010.[250] Japanese fighter jets scrambled a record of over 300 times in the area the next year. This is dangerously dry tinder for escalation[251] between a key U.S. ally and a nuclear-armed, rising China. U.S. diplomats have struggled to balance their neutrality in the dispute over the islands' ownership, with a strategy to protect U.S. interests that combines reassuring Japan and deterring China. But Washington's analysis of the issue misses a core challenge

---

[249] Adapted from Nicholas D Wright and James L. Schoff, "China and Japan's Real Problem: Enter the Fairness Dilemma," *The National Interest*, November 2, 2014.
[250] Schoff, J. L. (2014). Obama's Quiet Priority in Japan: The East China Sea. Retrieved January 24, 2019, from https://carnegieendowment.org/2014/04/10/obama-s-quiet-priority-in-japan-east-china-sea-pub-55311
[251] Goldstein, A. (2013). First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations. *International Security*, *37*(4), 49–89.

in Japan-China relations that increases the risk of conflict: a fairness dilemma (Box 6.1).

6.4.   Many U.S. policy-makers view the rise of Japan-China tensions through the lens of a security dilemma between the two, where each side's fear of the other side's capabilities and uncertain intentions leads to countermeasures that feed a vicious cycle.[252] Policies to address a security dilemma include reassuring allies while reducing uncertainty through transparency and clear deterrence. Reducing this fear is necessary, but insufficient in this case.

6.5.   A realistic view of human decision-making describes another fundamental driver of potential tragedy in East Asia: fairness. Some think fairness and justice "ought" to matter for moral or religious reasons. But modern biology tells us that rejecting unfairness *is* a deep-rooted biological drive, for which humans are prepared to pay large costs – fairness matters as an "is" not just as an "ought."

6.6.   For U.S. policy-makers, fairness matters because it *is* a powerful motivation for both China and Japan. Yet these countries' perceptions of fairness are often incompatible, leading to a fairness dilemma that could end in tragedy and draw in the U.S. military. Between China and Japan now, the standard playbook of reassurance and resolve are necessary but not enough. A strategy taking into account the fairness dilemma, however, could just work in such a Grey Zone arena.

Fairness: from "ought" to "is"[253]

6.7.   Humans are prepared to reject unfairness at substantial cost, and this is rooted in our biology. In a classic example called the ultimatum game, one individual gets an amount of money (e.g. $10) and proposes a split with a second player (e.g. $9 for herself, $1 for the second person). The other individual then decides whether to accept the offer (in which case both get the split as proposed) or reject the offer (in which case both players get nothing). Despite receiving an offer of free money, the second player rejects offers involving less than 25 percent of the money around half the time.[254] Even non-human primates reject unfairness. Capuchin monkeys performing a simple job reject payment of cucumber (which they like) when for the same job a fellow monkey gets tasty red grapes.[255] In essence, unfairness has a negative value that outweighs the positive value of the money (or cucumber) they would otherwise receive.

6.8.   Neural activity reflects the precise degree of unfairness in social interactions, including the game described above. Further, scientists are developing detailed knowledge of how this occurs even within brain regions. The drive to reject unfairness is a powerful motivation in decision-making, and it is often how nations end up in lose-lose situations.

6.9.   Pioneering realist Hans Morgenthau understood that a realistic view of human decision-making matters. At the start of *Politics among Nations* he wrote, "This theoretical concern with human nature as it actually is, and with the historical

---

[252] Thomas J. Christensen, "China, the U.S.-Japan Alliance, and the Security Dilemma in East Asia," *International Security* 23, no. 4 (April 1, 1999): 49–80.

[253] Adapted from Wright and Schoff, "China and Japan's Real Problem."

[254] Camerer, *Behavioral Game Theory*.

[255] S. F Brosnan and F. B.M De Waal, "Monkeys Reject Unequal Pay," *Nature* 425, no. 6955 (2003): 297–299.

processes as they actually take place, has earned for the theory presented here the name of *realism*." [italics his]

6.10.   But while Morgenthau privileged the concept of interest defined in terms of power, and this clearly matters in Grey Zone competition—such as between China and Japan—the tensions between them involve more than power and fear.

6.11.   Morgenthau's first principle of political realism emphasized that politics is governed by objective laws with their roots in human nature.[256] In this observation he echoes the father of realism – Thucydides – who suggested in the 5th Century BC a trio of human drives behind war including honor, fear, and self-interest.[257] Neither Thucydides nor Morgenthau had the tools available to understand human motivations (such as honor) beyond observation, but their origins and effects are becoming increasingly predictable. As modern science clarifies the neurobiology underlying human nature, diplomats and defense planners should update their strategies for managing various types of conflict. This will include considering perceptions of fairness as something that "is" crucial to foreign policy success, not just a factor that "ought" to be important.

6.12.   Understanding fairness as an "is" rather than an "ought" matters practically. Consider deterrence.

Fairness can limit deterrence and cause escalation

6.13.   Understanding fairness can help analysts interpret and forecast others' decisions more accurately. For instance, deterrence analysis that ignores the drive to reject unfairness can't correctly forecast what is needed for actions to be deterred – such as over the Senkaku/Diaoyu islands. How this affects deterrence is shown by considering the central concept in the U.S. Deterrence Operations Joint Operating Concept (DO JOC, 2006 v2). Figure 6.1 shows how in the DO JOC the other chooses between two options (to act or show restraint) based on the costs and benefits associated with each. Figure 6.1 then shows how in the ultimatum game in the other chooses between two options (to reject or accept) based on the costs and benefits associated with each – but, crucially, correct forecasting of behavior must include the value of fairness that drives them to reject. Now consider the DO JOC again, and see that when conducting a deterrence operation the social motivation of fairness may drive them to reject restraint, so deterrence fails.

---
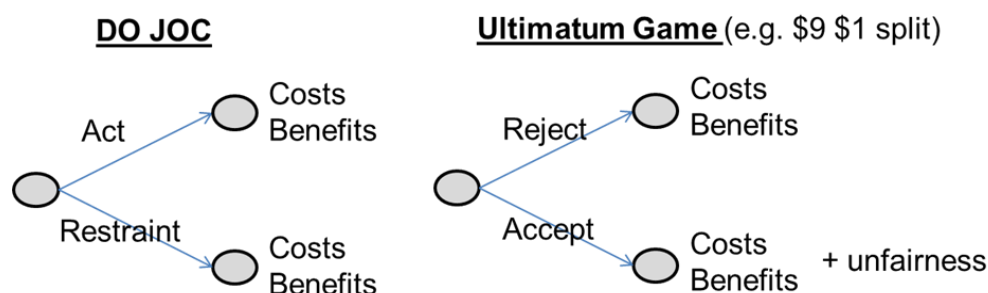
[256] Hans Morgenthau, Kenneth Thompson, and David Clinton, *Politics Among Nations*, 7 edition (Boston: McGraw-Hill Humanities/Social Sciences/Languages, 2005).
[257] Donald Kagan, *On the Origins of War: And the Preservation of Peace* (New York: Anchor, 1996).

Figure 6.1: Fairness can limit deterrence and cause escalation

6.14. The motivation to reject unfairness and the humiliation from unfair treatment—even at substantial cost—can form a central part of national narratives, and is reflected in national decision-making. In a powerful Chinese narrative, mostly Western powers imposed "Unequal Treaties" on a weak China in the nineteenth Century These treaties unfairly exploited China's weakness, leading to a "Century of Humiliation."[258] This cultural narrative instills a sense of entitlement to recover and receive restitution for past losses. Such beliefs may have played a role in the Chinese border clash with the Soviet Union in 1969, where scores died on both sides and nuclear threats were levelled.[259] The Chinese were motivated in part by the desire to revise one of the old Unequal Treaties with Russia – the 1860 Treaty of Peking. The Soviets had refused the Chinese request four years before to recognise it as an unequal treaty. And the specific objection was how to split the uninhabited, useless islands in the river Ussuri between the two countries: the Soviets wanted them all, the Chinese an equal split. It was the Chinese who initiated the military confrontation despite overwhelming Soviet nuclear and local conventional superiority.

6.15. Contemporary Iran has not been deterred from continuing to develop its nuclear programme, despite costs over $100 billion.[260] As Iranian Foreign Minister Javad Zarif asked in a Youtube message during the nuclear negotiations: "Imagine being told that you cannot do what everyone else is doing. Would you back down? Would you relent? Or would you stand your ground?"[261]

6.16. This social motivation can shape the specific form of events during a crisis. For example in 2001 a U.S. EP-3 reconnaissance plane and a Chinese fighter collided, which led to the loss of the Chinese pilot and forced the U.S. plane to land on Hainan in China. The key Chinese demand was for an apology.[262]

Policy implications of four aspects of fairness
(a) Distributional fairness: This relates to unfair distributions of punishments and rewards between people or groups. This matters because: (i) need to understand the motivations of potential criminals or armed political actors to deter them; and (ii) must also anticipate when key audiences perceive their actions as unfair, because this may lead to rejection of their actions that reduces their legitimacy. How much will key audiences perceive that events reflect unequal treatment of people/groups? *Recommendation:* Practitioners should ask: *"How fair did the audience understand the event to be?"*

[258] Zheng Wang (2012) *Never Forget National Humiliation: Historical Memory in Chinese Politics and Foreign Relations* (New York: Columbia University Press).
[259] Gerson, *The Sino-Soviet Border Conflict*.
[260] Wright and Sadjadpour, "The Neuroscience Guide to Negotiations With Iran."
[261] Javad Zarif, *Iran's Message: There Is A Way Forward*, 2013, http://www.youtube.com/watch?v=Ao2WH6GDWz4&feature=youtube_gdata_player.
[262] Swaine, Zhang, and Cohen, *Managing Sino-American Crises*.

(E.g., were recent similar actions by those in another group not punished; and if the action was a response, how far was it perceived as proportional?)
(b) Procedural fairness: Was the action *performed* in an unfair way? E.g., as in any policing, did the audience perceive that appropriate procedures were followed? *Recommendations:* Justice should be seen to be done. Provide information on procedures. Provide easily accessible justifications of the fairness of the decision-making process. Provide adequate complaints procedures that avoid overly bureaucratic and legalistic language.
(c) Horizontal and vertical inequality: In addition to inequality between richer and poorer members of a society (vertical inequality), there can also be inequality between groups or factions in a society (horizontal inequality). Both matter. *Recommendation:* Understand that people may reject perceived unfair treatment of their group, even if this reduces overall inequality in society. Thus, giving material incentives (or withholding punishments) to other groups may be counterproductive.
(d) Fairness is subjective: (i) Fairness often causes discord, because what is fair from the various parties' perspectives can be incompatible. This can lead to a Fairness Dilemma. (ii) Furthermore, simply considering inequality does a bad job of predicting armed unrest or insurgency[263] – what matters is the perception of unfairness. What affects perceived fairness? Flamboyant corruption or unfairness that is highly visible and salient. Another factor is how rapidly the inequality changes, as more unexpected inequality has more impact. *Recommendation:* Practitioners should ask: *"How visible or unexpected is this inequality for the audience?"*

Table 6.1: Policy implications of four aspects of fairness

BOX 6.1: THE FAIRNESS DILEMMA AND HEGELIAN TRAGEDY BETWEEN CHINA AND JAPAN[264] Danger between Japan and China arises not just from their military investments or rules of engagement, but also from their mutually incompatible subjective perceptions of the fairness of each other's' positions. This fairness dilemma can lead to the type of tragedy identified by the philosopher Georg Hegel, where tragedy does not arise from the clash of right and wrong, but instead because each side firmly believes itself right. Moreover, justice demands punishment or rejection of the other's action that is perceived as unfair. Two sources fuel the current fairness dilemma between China and Japan: their historically-based narratives; and their contemporary conceptions of what constitutes fairness in the international system.

---

[263] Sambanis, Schulhofer-Wohl, and Shayo, "Parochialism as a Central Challenge in Counterinsurgency."
[264] Adapted from Wright and Schoff, "China and Japan's Real Problem."

Consider a Japanese narrative. Imperialism was rampant before and during the Pacific War (World War II). Japan behaved little differently to other colonial powers, but had the misfortune to begin late and lose the war. They were severely punished by the firebombing of Tokyo and nuclear attacks killing an estimated 280,000;[265] destruction of up to one-third of the nation's wealth[266]; imposition of a war-renouncing constitution; de-deification of the Emperor; redistribution of lands; and Allied war crimes trials that resulted in about 920 executions of Japanese with some 3,000 more by the Soviets.[267] Japan apologized at various times for the War and related regional suffering, including by Prime Minister Yasuhiro Nakasone in 1985 and Emperor Akihito in 1990. Prime Minister Murayama's 1995 statement on the war apologized for Japan's "aggression and colonial rule," and in 1993 Chief Cabinet Secretary Yohei Kono apologized on behalf of the Japanese government for its role in coercively recruiting wartime prostitutes ("comfort women") and the "immeasurable pain and incurable physical and psychological wounds" they suffered. Japan paid reparations (in different forms) to occupied countries under the 1951 San Francisco Peace Treaty, and to South Korea and China under their 1965 and 1972 treaties respectively; treaties that officially settled war-related legal claims between the governments and their people. From the perspective of most Japanese, the country reflects on history as well as most others, and any concern that Japan might revert to its militarist past simply ignores its current political, legal, and societal reality.

Then consider a Chinese narrative. China ridicules the idea that Japan was "just another imperial power" in the 19th Century and sees it as a pitiless aggressor. Moreover, Japan has frequently sought to downplay and obfuscate its wartime aggression that caused millions of Chinese civilian deaths,[268] whether it is in the form of opinion leader commentary or through its education system. Emblematic of this aggression and insufficient contrition is the 1937-38 "Nanjing Massacre" in which Japanese forces murdered about 300,000,[269] but that some influential Japanese politicians and commentators deny happened.[270] Even before this, in the nineteenth century Japan had joined the pack of Western powers to force "Unequal Treaties" on China that unfairly exploited her weakness, leading to the "Century of Humiliation" and significant territorial losses including Taiwan and several islands. As for the post-War occupation of Japan, although the United States initially took a punitive approach, Washington eased up considerably as the Cold War intensified and released many former war criminals who assumed positions of power. In addition, Japan's alliance with the U.S. and Europe conspired over the years to write rules of international law and finance to their advantage. Now that China recovered its strength (after much toil and great cost), they demand that Beijing conform completely to these so-called international norms. There is a powerful sense of entitlement to recover and receive restitution

---

[265] United States Strategic Bombing Survey. (1946). *Summary report (Pacific war) Washington, D.C., 1 July 1946.* Washington : U.S. Govt. Print. Off. Retrieved from http://archive.org/details/summaryreportpac00unit
[266] Dower, J. W. (1999). *Embracing Defeat: Japan in the Wake of World War II.* W.W. Norton & Company/New Press.
[267] Ibid.
[268] Mitter, R. (2013). *Forgotten Ally: China's World War II, 1937-1945* (1st edition). Boston: Houghton Mifflin Harcourt.
[269] Yang, D. (1999). Convergence or Divergence? Recent Historical Writings on the Rape of Nanjing. *The American Historical Review*, *104*(3), 842–865. https://doi.org/10.2307/2650991
[270] BBC. (2014, February 4). NHK governor denies Nanjing massacre. Retrieved from https://www.bbc.com/news/world-asia-26029614

for past losses, as well as to establish new legal and diplomatic relationships more reflective of the current regional power dynamics.

Compounding these incompatible, historically-based narratives are very different contemporary conceptions of what constitutes fairness in the international system. To Japan the rule of law is of primary importance. For instance, Japan may not agree with the 2014 ruling against the country's whaling practices by the International Court of Justice, but it plans to abide[271] by the ruling, consistent with its narrative. Indeed, even at times of relative strength in the 1930s or the 1980s, Japan regularly justified its foreign and trade policies by citing international law.

In contrast, China often views fairness and justice in a historical context and in terms of the nation's sovereign rights, which can together outweigh the letter of the law. This helps justify China's repeated incursions into the territorial waters of the Japanese administered Senkaku/Diaoyu islands. Beijing believes it has historical claim.[272] And Beijing believes that because Japan is using its administrative control over the islands to establish de facto sovereign ownership,[273] therefore given China's rights it is fair for China act more assertively than the letter of law may permit. It is not necessarily that China believes "might makes right," but that China's increased strength[274] now allows it to accomplish what it believed to be "right" all along. A key Japanese concern is whether China's perception of "what's right" will be elastic in connection with its growing power.

These narratives and conceptions of fairness are compelling when seen from within each country – but they are incompatible.

LEGITIMACY

6.17.   Legitimacy is key at the level of interacting states. The perceived legitimacy of their actions was, for instance, a serious concern to all major European powers in the crisis immediately preceding World War I. Legitimacy also matters at the level of populations within states, such as within the Ukraine. I discuss five aspects of legitimacy below.

---

[271] Reuters, S. (2014, April 1). Australia welcomes court order on Japan whaling – video. *The Guardian*. Retrieved from https://www.theguardian.com/world/video/2014/apr/01/australia-welcomes-whaling-decision-video
[272] International Crisis Group. (2014, July 24). Old Scores and New Grudges: Evolving Sino-Japanese Tensions. Retrieved January 25, 2019, from https://www.crisisgroup.org/asia/north-east-asia/china/old-scores-and-new-grudges-evolving-sino-japanese-tensions
[273] International Crisis Group. (2013, April 8). Dangerous Waters: China-Japan Relations on the Rocks. Retrieved January 25, 2019, from https://www.crisisgroup.org/asia/north-east-asia/china/dangerous-waters-china-japan-relations-rocks
[274] Ibid.

6.18. **First, legitimacy is critically a matter of perception;** it is subjective. In defining legitimacy the scholar Francis Fukuyama, for instance, notes how "Legitimacy represents a broadly shared perception that certain social arrangements are just."[275]

6.19. **Second, perceived legitimacy by key audiences is key to keeping Grey Zone actions limited.** Henry Kissinger described its importance at the interstate level.[276] He describes how legitimacy "…implies the acceptance of the framework of the international order by all major powers, at least to the extent that no state is so dissatisfied that, like Germany after the Treaty of Versailles, it expresses its dissatisfaction in a revolutionary foreign policy. A legitimate order does not make conflicts impossible, but it limits their scope."

6.20. **Third, legitimacy is a source of influence**, which the U.S. and allies must attempt to harness. This is seen in the work of diverse scholars. Harvard's Arthur Applbaum who works on democratic leadership writes that "…legitimacy is a kind of moral power, the power to create and enforce nonmoral (or perhaps I should say not yet moral) prescriptions and social facts. A legitimate authority has the moral power to author legal, institutional, or conventional rights and duties, powers, and liabilities, and create social facts and mechanisms of coordination that change the legal, institutional, and conventional situation or status of subjects. [277]

6.21. Tom Tyler has conducted seminal work on US domestic policing. He writes that "Legitimacy is an internal value that is linked to personal feelings of obligation and responsibility to others." He goes on that "…legitimacy derives from judgments about how those others exercise authority, judgments not based upon the favorability or even the fairness of the decisions the authorities make, but upon beliefs about what are fair or ethical procedures for exercising authority. Hence, the exercise of authority via fair procedures legitimates that authority, and encourages voluntary deference."[278]

6.22. In international relations, as scholar Christian Reus-Smit writes, "Legitimacy is a quality that society ascribes to an actor's identity, interests, or practices, or to an institution's norms, rules, and principles. When society ordains this quality, such things are said to enjoy or command legitimacy."[279]

6.23. **Fourth, legitimacy is not simply synonymous with legality** – unlike in some particularly American or British conceptions derived from the emotionally powerful narrative about those countries' constitutional histories. Whilst the Oxford English dictionary, for instance, defines legitimacy as "the condition of being in accordance with law or principle"[280], other definitions note legitimacy requires far more than law as a number of scholars describe. Richard Merelman writes that "Legitimacy is a quality attributed to a regime by a population. That quality is the outcome of the government's capacity to engender legitimacy." "…political legitimacy as the quality

[275] Fukuyama, F. (2014). Political Order and Political Decay: From the Industrial Revolution to the Globalisation of Democracy. 1st ed. London: Profile Books. p.41

[276] Kissinger, H. A. (1957). A World Restored. Boston: Houghton Mifflin. pp.1-2

[277] Applbaum, A. I. (2010) "Legitimacy without the Duty to Obey." Philosophy and Public Affairs 38 (3): 215–39. p.221

[278] Tyler, T. R. (2006). "Psychological Perspectives on Legitimacy and Legitimation." Annual Review of Psychology 57: 375–400. Quotes from pp. 390 and 394

[279] Reus-Smit, C (2007) "International Crises of Legitimacy." International Politics 44: 157–74. p.159

[280] Murray, J.A.H. (1971). The Compact Edition of the Oxford English Dictionary. Compact edition. Vol. 1. 2 vols. Oxford University Press.

of "oughtness" that is perceived by the public to inhere in a political regime."[281] For David Easton, legitimacy is "the conviction on the part of the member that it is right and proper ... to accept and obey the authorities."[282] The famous Seymour Lipset wrote: "Legitimacy of the political system is its capacity to engender and maintain the belief that the existing political institutions are the most appropriate ones for the society."[283]

6.24.   **Fifth, the legitimacy of security arrangements often undergo a process of evolution.** The character of the process matters deeply, with an analogy here being the importance of "procedural fairness" described above – that a thing is done fairly. As Virta and Branders note when analysing the case study of Finland "Democratic political systems, representative democracy and the networked governance of security are not self-evident building blocks for legitimate security. They do not guarantee the legitimacy of security policymaking and implementation processes. The source of legitimacy is not the predetermined will of citizens but rather the process of its formation—that is, genuine political deliberation itself."[284]

6.25.   Moreover, the end point of the evolutionary process can be at least partly unintended. Baum and McGahan[285], for instance, investigated the emergence of the private military and security industry since the end of the Cold War. Despite its controversial nature, the industry achieved sufficient legitimacy since the end of the Cold War to account at times for the majority of military personnel deployed in Afghanistan and Iraq. They describe a drift from state's more unique ability to use force, to one where sometimes the industry may even be deemed more legitimate and morally acceptable.

Box 6.2: Russia and the use of legitimacy in the Grey Zone

Russia in Crimea, March 2014

Within a series of events, on 27 February 2014, pro-Russian gunmen seized the Crimean parliament. Emmanuel Karagiannis[286] discusses how within Russia the annexation was legitimised using Russian nationalism, Crimea returning "home" and that the annexation was seen as correcting a historical mistake.

President Putin in his speech on 4th March 2014 legitimized the intervention in Crimea on the two premises. First, the overthrow of Ukrainian President Yanukovych lead to a nationalistic government that threatened the ethnic Russian population in Crimea – and thus Russia intervened following the legitimate Ukrainian president's appeal to 'protect the lives, freedom, and health of the

---

[281] Merelman. R. M. (1966). "Learning and Legitimacy." American Political Science Review 60 (3): 548–61. doi:10.2307/1952970. p.548

[282] Easton, D. (1965). A Systems Analysis of Political Life. Wiley. p.278

[283] Lipset. S. M. (1959). "Some Social Requisites of Democracy: Economic Development and Political Legitimacy." The American Political Science Review 53 (1): 69–105. p.86

[284] Virta, S. and Branders M. (2016). "Legitimate Security Understanding the Contingencies of Security and Deliberation." British Journal of Criminology 56 (6): 1146–64.

[285] Baum, J. A. C. and McGahan, A. (2013) "The Reorganization of Legitimate Violence: The Contested Terrain of the Private Military and Security Industry during the Post-Cold War Era." Research in Organizational Behavior 33:

[286] Karagiannis, E. (2014). "The Russian Interventions in South Ossetia and Crimea Compared: Military Performance, Legitimacy and Goals." Contemporary Security Policy 35 (3): 400–420.

citizens of Ukraine'. Second, Russia had to take pre-emptive measures in Crimea, because of the threats to local Russian forces from armed Ukrainian nationalists. On 18th March Putin noted the analogy of Western intervention in Kosovo. Foreign Minister Lavrov also compared Russia and Crimea to other countries and territories – the UK and the Falklands, as well as France and the Comoros. As Putin said on 4th March: "we are often told our actions are illegitimate, but when I ask, 'do you think everything you do is legitimate?' they say 'yes'. Then, I have to recall the actions of the United States in Afghanistan, Iraq, and Libya".

Russia and Georgia in South Ossetia, August 2008

The intervention in South Ossetia was Russia's first war against a sovereign state in the post-Cold War period. Russian strategy for legitimacy involved two key aspects. First, one aspect of the Kremlin's strategy was to emphasize peacekeeping obligations when the breakaway republic was attacked by Georgian troops. As the scholar Karagiannis describes[287], under the 1992 Sochi Agreement on the Settlement of the Georgian–Ossetian Conflict, the Joint Control Commission was established to guarantee the ceasefire and monitor the situation in the conflict zone. Secondly, Russia used previous Western actions in Kosovo as a justification, and accused Georgia of genocide against the local population, as well as arguing that military operations would defend Russian peacekeepers in South Ossetia. Moreover, the Russian leadership utilized Kosovo as a legal precedent for *de jure* recognition of Abkhazia and South Ossetia.

STATUS: A SOURCE OF INFLUENCE

6.26.   Status is a powerful motivation at the both the State and Population levels – and can be used as a source of influence with both Populations and States.

6.27.   Status matters at the Population level, as shown by the experimental evidence described below (and in Appendix 1) as well as real-world examples like its role driving recruits to the Taliban.[288] Cognitive scientists have extensively studied social status, and typical definitions are: "…status, defined here as social respect, recognition, importance, and prestige"[289]; or "…status refers to the evaluation of where a given target stands with regard to whatever the bases of respect or esteem may be."[290]

6.28.   The role of status driving States' behaviour is shown across diverse historical cases, such as Russia and China.[291] Reviewing Chinese foreign policy, David Shambaugh argues that status accounts for key aspects of Chinese diplomatic behaviour, such as

---

[287] Ibid.

[288] Munoz, A. (2012). U.S. Military Information Operations in Afghanistan. Rand Corp.

[289] Fiske, S.T. (2010). "Interpersonal Stratification. Status, Power, and Subordination." In Handbook of Social Psychology, illustrated, 2:1464. John Wiley & Sons. p.941

[290] Cheng, J.T., Tracy J.L. and Anderson C. (2014). The Psychology of Social Status. Illustrated. Springer. p.74

[291] Larson, D. W., & Shevchenko, A. (2010). Status seekers: Chinese and Russian responses to US primacy. *International Security*, *34*(4), 63–95.

"face diplomacy."[292] Discussing China, Yong Deng writes that "Status is about state's concerns over its material wellbeing and international treatment with the goal to engineer mutually reinforcing growth in both." and he argues that "China's struggle for status has been a struggle for great-power recognition by balancing acceptance and autonomy, compliance and revisionism, power and legitimacy, and globalisation and nationalism."[293]

Using status as a source of influence

6.29.   Status can also be used as a source of influence.

6.30.   **State level:** "Social creativity" has been suggested to manage competition over status, in which problems are reframed and different states achieve status in different fields.[294] One might militarily powerful, a champion of tolerance, or most pious.

6.31.   **Population Level:** Status has been used to influence behavior, as Appendix 1 describes in more detail (section on Audiences). One example is salespeople in a U.S. company who traded off approximately $30,000 in income to achieve membership in the firm's "club" for top performers.[295] Status awards may be especially useful when the quality of individual outputs is difficult to measure precisely.

HONOUR

6.32.   The final motivation in this constellation is honour. Honour may be considered the quality of knowing and doing what is morally right.[296] As the founding father of sociology, Max Weber, noted[297] "A nation will forgive damage to its interests, but not injury to its honour and certainly not when this is done in a spirit of priggish selfrighteousness."

6.33.   Recent work into the causes of conflict highlight honour. In particular, scholar Ned Lebow writes that "The changes in norms, values and the whole decision-making process in world politics may be influenced by irrational motives: appetite, spirit, fear and reason. Spirit is the strongest motive in IR, closely connected to the self-esteem of the leader and of the nation as a whole. Honour and standing are instruments of achieving higher self-esteem and thus, one of the crucial causes of war. The nature of honor makes it a zero-sum game."[298] Lebow notes the Ancient Greek definition of honour: "Honor (timē) – a status that describes the outward recognition we gain from the others in response to our excellence." "Honor is also a mechanism for restraining

---

[292] Shambaugh, D. (2013). *China goes global: The partial power*. Oxford University Press

[293] Yong, D. (2008). *China's Struggle for Status: The Realignment of International Relations*. Cambridge University Press. p. 2

[294] Larson & Shevchenko (2010); Wohlforth, W. C. (2009). Unipolarity, status competition, and great power war. *World Politics*, *61*(01), 28–57.

[295] Larkin, I. (2011). Paying $30,000 for a gold star: An empirical investigation into the value of peer recognition to software salespeople. *Mimeo*.

[296] Murray, J.A.H. (1971). The Compact Edition of the Oxford English Dictionary. Compact edition. Vol. 1. 2 vols. Oxford University Press.

[297] Weber, M (2004). The Vocation Lectures / Max Weber : "Science as a Vocation", "Politics as a Vocation" ; Edited and with an Introduction by Owen, D.S. and Strong, T.B.; Translation by Livingstone, R. Indianapolis : Hackett Pub. p.80

[298] Lebow, R.N.. 2008. A Cultural Theory of International Relations. Cambridge University Press. p.64

the powerful and preventing the kind of crass, even brutal exploitation common to hierarchies in modern, interest-based worlds. Honor can maintain hierarchy because challenges to an actor's status, or failure to respect the privileges it confers, arouse anger that can only be appeased by punishing the offender and thereby "putting him in his place." Honor worlds have the potential to degenerate into hierarchies based on power and become vehicles for exploitation when actors at the apex fail to carry out their responsibilities or exercise self-restraint in pursuit of their own interests."[299]

6.34.   Policymakers must anticipate that others will be driven by honour – such as not backing down in the face of deterrent threats. One must, for instance, decide whether to provide adversaries with face-saving off-ramps.

RECOMMENDATIONS

6.35.   Fairness takes many forms and this drive should be included when analyzing an audience's decision calculus. See Table 6.2. It may mean *greater* deterrent threats are required than without anticipating this motivation. Strategies to minimise perceived unfairness may be needed to manage escalation of Grey Zone conflict.

6.36.   Legitimacy is a key battleground and should be actively planned for as a source of influence.

6.37.   Status should be used to help motivate individuals within populations, particularly where those individuals' outputs are difficult to measure.

---

[299] Ibid. p.65

Chapter 7: Norms and norm change – the neural phenomenon of "prediction error"

7.1.   Managing change is key to the international system. Change will always occur, for example from technological, demographic or economic drivers. Failure to manage change can lead to war.

7.2.   Norms are the "rules of the road" in the international system. Managing potential changes in norms is critical in the Grey Zone.

7.3.   The neural phenomenon of "prediction error" is critical to how humans change their expectations about the world – unexpected events that violate norms change those norms. Thus, the U.S. must manage unexpectedness and unpredictability in the Grey Zone. For instance:

> ➢ Breaking a norm can be deliberate, to shock. Soviet leader Nikita Khrushchev banging his shoe on the table in the UN. Chinese leader Deng Xiaoping hugging the prime minister of Japan. Sadam Hussein's use of chemical weapons. Syrian use of chemical weapons.
>
> ➢ Salami slicing and ambiguity can be used to change norms without causing significant prediction error and thus less psychological impact.

7.4.   This chapter first discusses what norms are and where they come from. Next, it discusses how international norms are thought to change. Finally, it discusses "prediction error", which provides a simple framework for anticipating key ways that Grey Zone actions may affect norms.

NORMS ARE THE "RULES OF THE ROAD"

7.5.   What norms are norms and where do they come from? International norms have a fundamentally psychological dimension, as discussed below, and so we first discuss the psychology of norms before going on to describe international norms.

7.6.   **The psychology of norms and norm change:** Norms in large part reflect our expectations about the environment. While the content of norms is culturally dependent, our basic human biology makes us norm-following animals because we use expectations of the world to understand the world.[300] Thus, norms come from the combination of nature and nurture. And how do these expectations change? When a norm is violated, this deviates from our expectation and this "prediction error" causes us to change our expectation, to change our norms, to change our expectation about the rules of the road. The bigger the "prediction error" associated with a norm violation, the bigger its psychological impact. As described below, "prediction error" is a crucial concept.

---

[300] Joiner, J., Piva, M., Turrin, C., & Chang, S. W. C. (2017). Social learning through prediction error in the brain. *Npj Science of Learning*, *2*(1), 8. https://doi.org/10.1038/s41539-017-0009-2; Sanfey, A. G., Stallen, M., & Chang, L. J. (2014). Norms and expectations in social decision-making. *Trends in Cognitive Sciences*, *18*(4), 172–174. https://doi.org/10.1016/j.tics.2014.01.011

7.7. **International norms in political science:** Many prominent definitions of norms in political science accord well with these psychological ideas – and indeed they contain crucial subjective or perceptual dimensions, so that applying ideas from modern cognitive science may help better understand them. To give an example, "Norms are defined as "intersubjective beliefs about the social and natural world that define actors, their situations, and the possibilities of actions" … They represent "shared expectations about appropriate behavior held by a community" that derive from a combination of beliefs, standards of behavior, international conventions, and decision-making procedures."[301]

7.8. In political science, however, norms can also often have an additional dimension related to what people *should* do ethically. Thus, "Norms appear to be many things to many people … One group of scholars thinks of international norms as modal forms of state behavior that have nothing to do with what is right or obligatory. Another group conceives of them as generalized standards of conduct that embody collective expectations about proper behavior."[302]

7.9. **International norms are built out of multiple materials:** Many scholars discuss the numerous forms that norms can take. To give one example: "International norms are typically defined as ideas of varying degrees of abstraction and specification with respect to fundamental values, organizing principles or standardized procedures that resonate across many states and global actors, have gained support in multiple forums including official policies, laws, treaties or agreements."[303] In another example, norms are "…a set of rules with a prescriptive character for a defined scope of application. Norms are codified through treaties or conventions, yet they can also be uncodified, as seen with customary rights. Within the international system, international norms regulate states' behaviour by enabling certain actions in accordance with the norm, and prohibiting other actions that may violate or juxtapose that norm."[304]

7.10. **International norm creation:** The creation of new norms will be particularly relevant with new technologies – as was seen with the creation of norms for nuclear weapons after World War II, or the current drive to establish norms for cyber (see Part III of this report on cyber). A key challenge is that this requires the involvement of multiple actors, who may be actual or potential adversaries. Norms are also importantly shaped by randomness and "path dependence", for example the QWERTY keyboard or driving on the left (in the UK) or right (in the US) side of the road.

7.11. Within these mechanisms, powerful states such as the US, China or Russia are particularly important. As one scholar writes[305], "For institutionalists, norms are embedded within international institutions and are therefore generated along with

---

[301] Lantis, J. S. (2011). Redefining the nonproliferation norm? Australian uranium, the NPT, and the global nuclear revival. *Australian Journal of Politics & History*, *57*(4), 543–561. Quoting Wendt, A. (1995). Constructing International Politics. *International Security*, *20*(1), 71–81. https://doi.org/10.2307/2539217

[302] Raymond, G. A. (1997). Problems and Prospects in the Study of International Norms1. *Mershon International Studies Review*, *41*(2), 205–245. pp. 216-7

[303] Krook, M. L., & True, J. (2012). Rethinking the life cycles of international norms: The United Nations and the global promotion of gender equality. *European Journal of International Relations*, *18*(1), 103–127. pp. 103-4

[304] Panke, D., & Petersohn, U. (2012). Why international norms disappear sometimes. *European Journal of International Relations*, *18*(4), 719–742. p. 721

[305] Hyde, S. D. (2011). Catch us if you can: Election monitoring and international norm diffusion. *American Journal of Political Science*, *55*(2), 356–369. p. 357

them, usually resulting from demand for interstate cooperation … Exactly how norms are created within institutions varies somewhat, but in many cases, collective action problems mean that powerful states help establish norms because of their disproportionate ability to set the agenda, offer side-payments, and reap the benefits of cooperation."

7.12. The ethical perspective of political scientists is also prominent in political science discussions, even if likely less so in the real world. Thus, "In the most widely cited theory of norm creation, social constructivists focus on norm entrepreneurs who, motivated by principled ideas, seek to change international or domestic behavior through the generation of new international norms."[306]

INTERNATIONAL NORM CHANGE

7.13. Crucial to managing Grey Zone competition, however, is how these international norms change over time. Indeed, changing existing norms may be the aim of some Grey Zone actions. Two key observations here are that international norms are constantly evolving and that challenges can change.

7.14. **International norms are constantly evolving:** As scholar Wayne Sandholtz describes, "Systems of rules or norms cannot be static; tensions between norms and behavior, and between different norms, drive a constant process of norm development. In every social system, the evolution of norms thus follows a cyclical, or dialectical, pattern."[307]

7.15. **Norm change in response to challenges to the norm:** Panke and Petersohn[308] write that "The effect of norm challenges varies. A norm may survive despite instances of non-compliance and despite the efforts of actors to delimit a norm through renegotiations" "The first and necessary step to undermine or abolish an embedded norm is that the norm be 'challenged', either because a state seeks to avoid compliance-costs, or desires to adjust the norm to changed considerations of appropriateness of new interests. Irrespective of motivation, norms can be challenged in several ways, for example explicitly, implicitly, verbally or through actions. In any case, a challenge breaks with the common habitus, but does not necessarily result in norm weakening. The mechanisms of norm challenges are not always the same, but are influenced by the institutional context of the norm."

7.16. Moreover, as Vincent Keating writes, many prominent scholars have suggested that "By routinely violating the original norm and offering competing interpretations, the state can make it increasingly difficult for the norm to be reaccepted, particularly if it is willing to invest its military capacity to promote the new norm."[309]

---

[306] Ibid. referencing Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, *52*(04), 887–917.

[307] Sandholtz, W. (2008). Dynamics of international norm change: Rules against wartime plunder. *European Journal of International Relations*, *14*(1), 101–131. p. 103

[308] Panke, D., & Petersohn, U. (2012). Why international norms disappear sometimes. *European Journal of International Relations*, *18*(4), 719–742. pp. 4-5

[309] Keating, V. C. (2014). Contesting the International Illegitimacy of Torture: The Bush Administration's Failure to Legitimate its Preferences within International Society. *The British Journal of Politics & International Relations*, *16*(1), 1–27. p. 5

MANAGING NORM CHANGE: THE NEURAL PHENOMENON OF "PREDICTION ERROR"

7.17.   Thus international norms are subjective and they change – and understanding the neural phenomenon of "prediction error" gives U.S. policymakers a simple framework to anticipate *which aspects of actions will affect norms*. Table 7.1 summarises this framework and provides policy options.

7.18.   In addition to norm change, a prediction error framework forecasts widespread and important effects (inadvertent escalation, surprise, etc.) and simplifies existing strategic concepts so it can be operationalized without extra analytical burden.[310]

What are prediction errors?

7.19.   A core insight from neuroscience is that when we make an action, the impact it has on the other's decision-making is crucially modulated by the action's associated "prediction error".[311] This prediction error is simply defined as the difference between what actually occurred, and what the other expected. The bigger the associated prediction error, the bigger the psychological impact of the action.

Prediction errors and insider knowledge causing inadvertent norm change

7.20.   One reason that prediction errors matter is because they can cause inadvertent norm change. When any of us make actions, we have "insider knowledge" of our own actions. When we make actions we use our "insider knowledge" to help predict and cancel out the events they generate. So, to us applying a force it is largely predicted, but the recipient does not have such insider knowledge and so experiences a stronger impact. Thus in a confrontation between actors, each action in turn has a stronger impact on its recipient than its originator, causing inadvertent escalation. In summary, we predict the effects of our own actions, so they have more impact on the other than we understand, or perhaps intended.

---

[310] e.g., Wright N.D., 2014, SMA White Paper on Neuroscience and Deterrence, DoD Joint Staff.

[311] It is central to how humans understand, learn and decide about the world, from simple tasks [Niv, Y., & Schoenbaum, G. (2008). Dialogues on prediction errors. *Trends in Cognitive Sciences*, *12*(7), 265–272], to more complex social interactions [Behrens, T. E. J., Hunt, L. T., & Rushworth, M. F. S. (2009). The computation of social behavior. *Science (New York, N.Y.)*, *324*(5931), 1160–1164].

Helping U.S. policymakers understand the events' psychological impacts on others Core idea: Throughout conflicts and limited wars, an action's associated prediction error always affects that action's degree of impact on the decision-making of audiences.		
1	*When anticipating an event's psychological impact, ask: "How unexpected is the event from that audience's perspective?"* Specific instances include:	For the audience of interest, describe the event's associated prediction error from their perspective and how that changes its signaling impact.
	a. *Domain-specific effects*	Actions in certain domains are inherently less well understood and so give larger prediction errors. E.g. cyber actions.
	b. *Cross-domain responses*	Following an action, we tend to expect a response in a particular domain, so a response in a less expected domain causes more prediction error and impact. The domain an audience expects may relate to the original action's domain[312], previous promises to act in a certain way, or established behavioral patterns.
	c. *Geography*	Distant responses likely cause more prediction error.
	d. *Novelty and first times*	These cause increased prediction error.
2	*Manipulate predictability*	Signpost diplomatic or military moves a day before to reduce their impact (e.g. via backchannels); act without warning to increase their impact.
3	*Anticipate effects of "insider knowledge"*	Actions likely have greater impact on the recipient than you understand. This matters most when you have greater "insider knowledge" of your actions.
When receiving actions oneself Core idea: Prediction errors are unavoidable, so we must manage their effects on ourselves.		
1	*Manage effects of prediction errors*	Large impacts from prediction error on U.S. decision-makers should be considered when reacting.
2	*Learning*	Prediction errors are the best material to improve our models of the world.
Longer term aim for U.S. policymakers		
1	Reducing the amount of prediction errors that accumulate from all events over time (i.e. increasing predictability; creating order) is a central idea behind influential theories for gaining population support in challenging environments (e.g. David Kilcullen[313]).	

Table 7.1: Predictions errors and policy options

---

[312] E.g. in the Vietnam conflict the U.S. response to torpedo boat attacks was to attack that same boat class; Schelling, *Arms and Influence*, 1966.

[313] E.g. systems of competitive control are a central idea in Out of the Mountains (2013), which in the definition on page 126 are "the local armed actor that a given population perceives as best able to establish a predictable, consistent, wide-spectrum normative system of control is most likely to dominate that population and its residential area".

Prediction errors explain diverse impacts across diplomatic and military confrontations

7.21. A simple prediction error framework helps forecast an event's impact on an audience, and thus how much it will change norms from their perspective. One asks *"how unexpected was the event from that audience's perspective?"*

7.22. An important instance is shown in Fig. 7.1, where an event can either occur or not occur, and can either be expected or not expected. Strategic bombing illustrates different combinations of these effects. First, an event occurs and was not expected, so has a large associated prediction error. For example, First World War German air raids on London were small-scale, but being so unexpected had a large psychological impact and caused panic. Second, extrapolating from this, influential inter-war airpower theorists suggested powerful and recurrent bombing would psychologically paralyze an adversary causing rapid collapse. However, such recurrent bombing is well expected. For example, in the "Blitz" on London, recurrent bombing exerted far greater destructive power but had far less psychological impact than forecast. Third, an event is expected but doesn't occur, so this absence itself leads to large prediction error. For example, in the Vietnam War, U.S. campaigns bombed regularly and used pauses as a conciliatory signal.

	Event not expected	Event expected
Event occurs	a) Associated with prediction error	b) No prediction error
Event not occur	(trivial case)	c) Associated with prediction error

Figure 7.1: illustrating prediction errors (prediction error = actual event – expected event)

7.23. The nature of events can also be more or less unexpected, so that the prediction error associated with the event can increase or decrease its impact. Examples of this are shown in Table 7.1, including domain-specific effects and cross-domain effects, as well as effects related to geography, novelty and first times.

Prediction errors may be reduced by ambiguity and salami-slicing

7.24. Ambiguity and salami-slicing are key methods for reducing the impact of individual actions and so gradually changing norms over time without providing perceived grounds for significant responses in the eyes of key U.S. allies, domestic and other audiences. U.S. responses to such here may include enhancing the prediction error associated with such activities, for example by releasing large amounts of information intermittently to enhance its impact and by making the nature of the information released novel.

RECOMMENDATIONS

7.25.   Norms are the "rules of the road" in the international system – and in the Grey Zone U.S. policymakers should regard managing potential changes in norms as an end in itself.

7.26.   The U.S. must manage unexpectedness and unpredictability in the Grey Zone, because this is key to norm change. For example, breaking a norm can be deliberate, to shock and send a powerful signal; whilst salami slicing and ambiguity can change norms without causing significant prediction error and thus cause less psychological impact.

Chapter 8: Deterrence and escalation management

8.1.   Grey Zone conflict is necessarily limited – and thus an isolated focus on either deterrence or escalation management alone is insufficient. This chapter outlines a practical framework for influence, which incorporates both deterrence and escalation management. [314] Key points include:

- ➢ A realistic account of audience decision-making must lie at the heart of any influence strategy – as Part I of this report describes.
- ➢ Deterrence and escalation management are intimately related and are both cases of influence.
- ➢ Deterrence has a fundamentally cognitive dimension in both U.S. and Chinese doctrine.
- ➢ Escalation or de-escalation can result from events' predictability and unexpectedness. The U.S can manage this "prediction error."
- ➢ Controlling escalation involves not just minimising escalatory factors, but also positive accommodative and conciliatory gestures.
- ➢ Perceived fairness matters in shaping deals and deterrence (see Chapter 7).

8.2.   This chapter first describes how deterrence and escalation management relate and then examines both these cases of influence in more detail. I then note the significance of cross-domain influence. I discuss how to get to grips with culture. Finally, I emphasize three often overlooked factors in escalation management: prediction error, fairness and the importance of de-escalatory actions.

INFLUENCE

8.3.   I define influence as a means to affect an audience's behaviour, perceptions or attitudes. Influence can be achieved by deterrence, persuasion, or the use of hard or soft power. Influence does not only include "soft" means, but also the use or threat of hard power. Influence aims to affect an audience's decision process, which is shown in Fig. 8.1. The account of the audience's decision process used here is operationalizable for planning, for instance being entirely compatible with U.S. concepts such as the Deterrence Operations Joint Operating Concept (DO JOC).[315] To provide a focus for this chapter, I highlight two important cases of influence: deterrence and escalation management.

---

[314] I draw in particular here on Wright N.D., (2018) Mindspace: Cognition in Space Operations. Intelligent Biology; London. This companion publication is at www.nicholasdwright.com.
[315] US DoD, "Deterrence Operations Joint Operating Concept," *Version 2*, 2006.
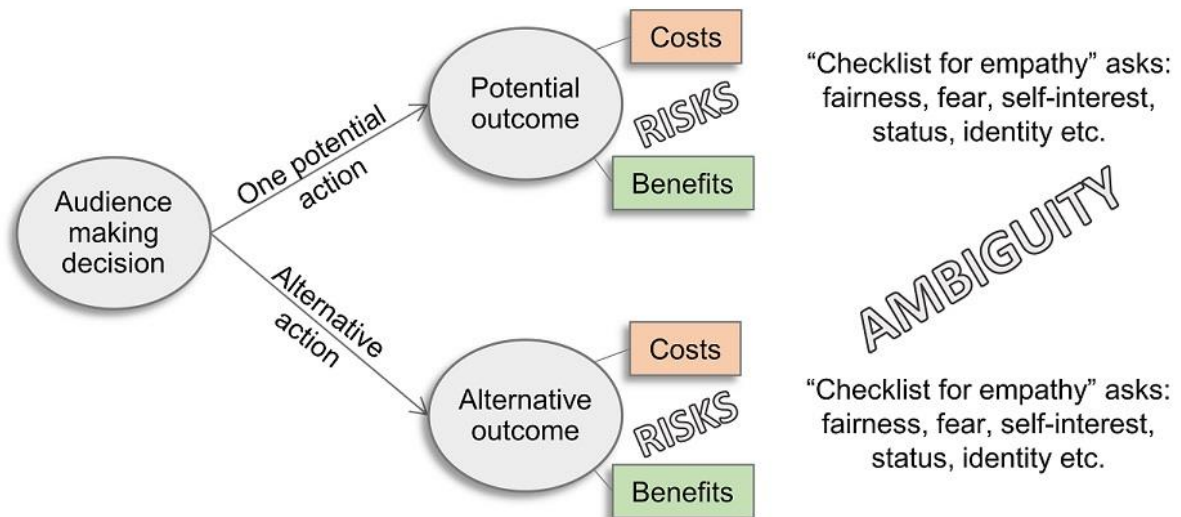
Figure 8.1: The Audience Decision Process. As Part I describes, the audience's decision calculus must be at the heart of planning for influence. Practical tools, based in evidence, can help put oneself in the audience's shoes (e.g. the "checklist for empathy").

HOW DO DETERRENCE AND ESCALATION MANAGEMENT RELATE?

8.4.   Deterrence and escalation management are intimately related and are both cases of influence.

8.5.   In U.S. thinking, deterrence is influencing an adversary so that they decide not to act rather than to act (see e.g. Fig. 8.2).

8.6.   Escalation can be defined as an increase in the intensity or scope of confrontation considered significant by one or more parties. We can consider three mechanisms of escalation: deliberate, inadvertent and accidental. [316] Escalation may be considered inadvertent when an actor's intentional actions are unintentionally escalatory. In deliberate escalation the degree of escalatory impact on the receiver was intended. In accidental escalation, the action itself was unintended. Management of inadvertent escalation is managing the influence of one's actions on the those receiving them. Management of deliberate escalation by the adversary involves deterrence.

8.7.   Deterrence and escalation management can work together and can be antagonistic. Actions taken in order to deter an adversary can contribute to escalation management, or may work against escalation management. How? If an adversary is deliberately escalating, then one can potentially deter further escalation by influencing the adversary's perceived cost/benefit judgement. However, if an adversary is escalating due to inadvertent escalation, then taking actions to deter the adversary through threatened punishment may make them fear further for their security and thus lead them to escalate further. It can escalate the spiral of tension between them.

---

[316] For discussion of such definitions see Forrest E. Morgan et al., "Dangerous Thresholds" (Rand, 2008).

8.8.   The scholar Robert Jervis neatly captured the tension between spirals and deterrence[317]: are we in the run up to World War I (where more defensively motivated actions led or contributed a spiral of fear driving towards war); or are we in the run up to World War II where we need to deter Hitler?

8.9.   Chinese thinking may be highly problematic with respect to such an understanding of escalation.[318] This arises because compared to much U.S. thought, Chinese strategic thinking considers escalation as more deliberate and controllable, and also considers signalling as more effective so that the message intended to be sent is the message that is received. Thus, if the Chinese believe escalation is much more the product of deliberate (rather than inadvertent) mechanisms, they will be much more likely to seek to deter that escalation and so worsen inadvertent escalation.

INFLUENCE: THE CASE OF DETERRENCE

8.10.   In U.S. thinking, deterrence is influencing an adversary so that they decide not to act rather than to act (Fig. 8.1). Deterrence may require that the adversary chooses not to act at all (e.g. this is standard in nuclear deterrence thinking) or they may only act at some acceptably low frequency (e.g. in some conventional applications or as seen in Israeli thinking[319]).

A fundamentally cognitive dimension to deterrence

8.11.   The cognitive foundation of deterrence is acknowledged by numerous U.S. and other Western official and scholarly documents.[320] One prominent U.S. DoD definition specifies that "Deterrence is a *state of mind* brought about by the existence of a credible threat of unacceptable counteraction" [emphasis mine][321]. The Deterrent Operations Joint Operating Concept also prominently states that "The central idea of the DO JOC is to decisively influence the adversary's decision-making calculus…."[322] Furthermore, as shown in Figure 8.2 above, which I adapt from the core concept and illustration in the DO JOC, the
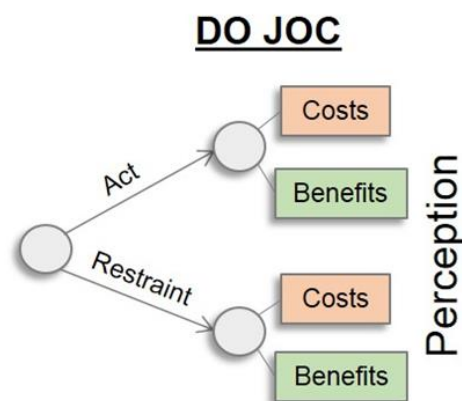
Figure 8.2: The adversary's decision calculus in the US DoD Deterrence Operations Joint Operating Concept (2006).

---

[317] Robert Jervis, *Perception and Misperception in International Politics* (Princeton: Princeton University Press, 1976).

[318] See below for further discussion and references.

[319] Mark Vinson, "An Israeli Approach to Deterring Terrorism," *PRISM Security Studies Journal* 5, no. 3 (2014): 61–75. Thomas Rid, "Deterrence beyond the State: The Israeli Experience," *Contemporary Security Policy* 33, no. 1 (April 1, 2012): 124–47, https://doi.org/10.1080/13523260.2012.659593.

[320] Wright ND (forthcoming) The Neurobiology of Deterrence: Lessons for U.S. and Chinese Doctrine in Eds. Knopf J and Harrington A "Behavioral Economics and Nuclear Weapons", University of Georgia Press

[321] Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02. This definition was present in the 1994 edition up to 2011, but not by 2016. it now defines deterrence as "The prevention of action by the existence of a credible threat of unacceptable counteraction and/or *belief* that the cost of action outweighs the *perceived* benefits" [emphasis mine].

[322] DoD, "Deterrence Operations Joint Operating Concept." p. 3

adversary's decision calculus is clearly shown as a decision between options (each of which has costs and benefits), and in which perception is key. The DO JOC goes on to state that "An adversary's deterrence decision calculus focuses on their perception of three primary elements: The *benefits* of a course of action; The *costs* of a course of action; The *consequences of restraint*" [emphasis in original].

INFLUENCE: THE CASE OF ESCALATION MANAGEMENT

8.12.   Escalation can be defined as an increase in the intensity or scope of confrontation considered significant by one or more parties. Escalation may be deliberate, inadvertent or accidental.[323] Escalation management has a fundamentally cognitive component for both deliberate and inadvertent escalation.

Managing deliberate escalation – a fundamental cognitive dimension

8.13.   Deterrence is the primary means to manage deliberate escalation. The cognitive dimensions of deterrence are discussed above.

Managing inadvertent escalation – a fundamental cognitive dimension

8.14.   Escalation may be considered inadvertent when an actor's intentional actions are unintentionally escalatory, that is the degree of escalation was not deliberate and the action was not accidental. I highlight three cognitive aspects below.

8.15.   Firstly, fear in action-reaction 'spirals'. 'Spiral' dynamics or the 'security dilemma' are invoked to explain many escalating peacetime action-reaction spirals of political hostility and military preparations[324], as well as inadvertent escalation during limited war.[325] Broadly speaking, such a spiral or security dilemma arises from fear or uncertainty of the other's motivations and capabilities, where precautionary or defensively motivated measures are understood or misperceived as offensive threats that can lead to countermeasures in kind.[326]

8.16.   Much scholarship places fear at the heart of action-reaction spirals.[327] As Robert Jervis wrote, 'to determine whether a security dilemma existed … one or both sides should have been deeply fearful that the other side was aggressive or would become so in the future.'[328] Or as Barry Posen concludes an analysis of the security dilemma, to understand the odds of conflict one must ask: "Which groups fear for their physical

---

[323] For discussion of such definitions see Morgan et al., "Dangerous Thresholds."

[324] Jervis, *Perception and Misperception*. Ch. 3 esp. pp. 62-76. Andrew Kydd, "Game Theory and the Spiral Model," *World Politics* 49, no. 3 (April 1997): 371–400, https://doi.org/10.1353/wp.1997.0012. Charles L. Glaser, "The Security Dilemma Revisited," *World Politics* 50, no. 1 (October 1, 1997): 171–201.

[325] Barry Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Cornell University Press, 1991). Chapter 1. Posen also discusses militaries' offensive bent and accidents, not covered here.

[326] Thomas J. Christensen, "China, the U.S.-Japan Alliance, and the Security Dilemma in East Asia," *International Security* 23, no. 4 (April 1, 1999): 49–80.

[327] Ken Booth and Nicholas Wheeler, *Security Dilemma: Fear, Cooperation, and Trust in World Politics*, First Edition (Basingstoke: Palgrave Macmillan, 2008). Ch. 3 for a review.

[328] Robert Jervis, "Was the Cold War a Security Dilemma?," *Journal of Cold War Studies* 3, no. 1 (January 1, 2001): 36–60, https://doi.org/10.1162/15203970151032146.

security and why?'[329] What 'fear' means varies widely: for some scholars being fundamentally biologically or psychologically with culture shaping its expression[330]; whilst for other scholars fear clearly matters but seems to fall out of rational explanations in terms of, for example, uncertainty over another's type.[331] However, at its core fear remains as an unpleasant emotion or apprehension caused by threat or danger.

8.17. Secondly, the thresholds over which an action is considered escalatory are fundamentally subjective – they exist in the minds of observers.[332]

8.18. Thirdly, the legitimacy or proportionality of reactions have a fundamentally subjective in the mind of the observer.[333]

CROSS-DOMAIN INFLUENCE

8.19. Managing the perceived proportionality and legitimacy of cross-domain actions and reactions during escalation is a tough challenge. I discuss this in a recent report on space operations.[334]

8.20. One further point concerns the limitations of the term "cross-domain deterrence", which has been an area of considerable recent scholarly interest. Given the cross-domain nature of many plausible escalation scenarios, as well as the interdependence of deterrence with escalation, I suggest instead examining the broader field of "cross-domain influence".

GETTING TO GRIPS WITH CULTURE – EAST ASIA AND THE WEST

8.21. In our globalized world, a key challenge when trying to put yourself in the shoes of others is how to get to grips with culture.

8.22. Does strategic thinking differ between China and the U.S.? Does what is common sense and intuitively plausible really differ between these cultures? Identifying such differences would help tailor influence strategies. Many influential voices argue that strategic thought differs between China and the West, rooted in millennia of cultural difference leading to different worldviews. Henry Kissinger wrote in *'On China'* that 'No other country can claim so long a continuous civilization, or such an intimate link to its ancient past and classical principles of strategy and statesmanship', and argued its cultural tradition shaped leaders such as Mao Zedong, Wen Jiabao and Hu Jintao.[335] The authoritative Chinese military textbook *The Science of Military Strategy*

---

[329] Barry R. Posen, "The Security Dilemma and Ethnic Conflict," *Survival* 35, no. 1 (1993): 27–47, https://doi.org/10.1080/00396339308442672.

[330] Booth and Wheeler, *Security Dilemma*. Ch. 3. Lebow Richard Ned, *A Cultural Theory of International Relations* (Cambridge University Press, 2008). p. 119.

[331] E.g. Andrew H. Kydd, *Trust And Mistrust In International Relations* (Princeton University Press, 2005). Fear is neither indexed nor clearly defined, but figures prominently. Part II is entitled 'Fear and the Origins of the Cold War' in which fear is central to Ch. 3 on 'The Spiral of Fear' and the subsequent historical descriptions. Charles L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation* (Princeton University Press, 2010). Again fear is not indexed or defined, but for example features in the description of signalling malign intentions pp. 70-1.

[332] Morgan et al., "Dangerous Thresholds."

[333] Schelling, Arms and Influence.

[334] Wright N.D., (2018) Mindspace: Cognition in Space Operations. Intelligent Biology; London.

[335] Henry Kissinger, *On China* (Penguin, 2011). Quote from p. 2, see also e.g. pp. 3, 103, 490.

states that 'The cultural tradition of all nations, especially the national cultural psychology has significance on the process of development of strategic theories.'[336]

8.23. But whilst it has been devilishly difficult to determine whether, and how, cultural differences affect behavior, in this report I apply robust findings from cross-cultural cognitive science. This provides an extra, independent source of evidence on cross-cultural differences, which I then explore further using consider cross-cultural analyses from doctrine, interviews and historical cases. I discuss cross-cultural factors further in Chapters 4 and 6.

8.24. Here, however, I first give the example of deterrence, which also highlights the significance of identifying commonalities as well as differences between cultures.

Chinese thinking on deterrence: commonalities and differences compared to the West

8.25. Chinese concepts of deterrence are broader and include both Western concepts of deterrence (influencing an adversary not to act) as well as compellence (influencing an adversary to choose to act rather than not act).[337]

8.26. However, as in the U.S. case above, Chinese doctrine also has cognition at the core of its thinking on deterrence. Chapter 9 in the authoritative PLA textbook *The Science of Military Strategy* is entitled "Strategic Deterrence." The authors write that "[D]eterrence requires turning the strength and the determination of using strength into the information transmitting to the opponent, and to impact directly on his mentality in creating a *psychological pressure* to shock and awe the opponent" [emphasis mine].[338] Elsewhere, this publication states, "There are three basic elements to carry out deterrence: First, appropriate military strength available; second, resolve and will to use force; and third persuading the opponent to perceive such strength and resolve."[339] Note that this was translated into English by the Chinese Academy of Military Sciences themselves--these are their own words and whilst one may argue that the Chinese use the term deterrence slightly differently to the U.S. literature (e.g. to include coercive diplomacy more broadly[340]), the broader point of the cognitive basis of their idea is clear.

8.27. Thus, despite the slightly wider Chinese scope, both Chinese and U.S. accounts consider deterrence as a form of influence, and both Chinese and U.S. accounts of deterrence contain important cognitive dimensions. In this Chinese case, this also accords with other characterizations of such Chinese concepts.[341] Furthermore,

---

[336] Guangqian Peng and Youzhi Yao, *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2005). p. 128.

[337] Schelling, *Arms and Influence*. Introduced this distinction within Western thinking.

[338] Guangqian Peng and Youzhi Yao, *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2005). See Ch 6 of this report for a discussion of challenges of identifying and interpreting Chinese doctrine.

[339] Peng and Yao. p. 18

[340] Li Bin, "China and Global Nuclear Arms Control and Disarmament," in *The War That Must Never Be Fought: Dilemmas of Nuclear Deterrence*, edited by George P. Shultz and James E. Goodby (Stanford, CA: Hoover Institution, 2015), p. 359; Dennis Blasko in Joe McReynolds, ed., *China's Evolving Military Strategy* (Brookings Institution Press, 2016).

[341] For example, Thomas J. Christensen writes that "It is fairly clear that deterrence, coercion, enemy psychology, and morale are key targets of many of the operations discussed in *Zhanyixue*" ("Coercive Contradictions: Zhanyixue, PLA Doctrine, and Taiwan Scenarios," in *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army*, ed. James C. Mulvenon and David Finkelstein

these Chinese and U.S. accounts also at least in part consider deterrence in terms of an account of the adversary's decision calculus, which includes the adversary's potential gains and losses from their alternative courses of action.[342]

THREE UNDER-EMPHASISED FACTORS IN GREY ZONE ESCALATION MANAGEMENT

8.28.   Finally, I note three significant factors for escalation management that are often overlooked, and so are important to highlight.

The neural phenomenon of "prediction error"

8.29.   Understanding prediction errors can help the U.S. decision-makers better understand events, to cause intended effects, and avoid unintended effects, on others in diplomatic or military confrontations. The previous chapter and Table 7.1 summarises policy options.

Fairness can lead to escalation or failure of deterrence

8.30.   The human drive to reject unfair behavior, even at great cost, can lead to escalation. Chapter 6 details this challenge.

Controlling escalation involves not just minimising escalatory factors, but also positive accommodative and conciliatory gestures

8.31.   The success of social animals such as humans crucially depends on their ability to dynamically manage the balance between cooperation and competition over time. A critical aspect of this is unilateral conciliatory or accommodative signals.

8.32.   Conciliatory gestures are natural and common: They are often needed to control escalation and enable de-escalation. The U.S. cannot understand crisis dynamics and how to control escalation without understanding conciliatory and accommodative gestures.

8.33.   Look for unilateral positive signals. It is true that flexibility may be mistaken for weakness, but both sides face this problem so it is important to look for them.

8.34.   Using prediction error can enhance conciliatory gestures: The cases in the section above on prediction error involve punishing events, but prediction errors equally apply to positive acts. Consider the Egyptian leader Anwar Sadat in 1977. Egypt lost two wars to Israel in 1967 and 1973, after which he made conciliatory efforts. But it

---

(Alexandria, VA: CNA Corp,.2005. Henry Kissinger, *On China* (Penguin, 2011). observes (pp. 133-35) that "Mao's actions in the Korean War require an understanding of how he viewed what, in Western strategy, would be called deterrence or even preemption and which, in Chinese thinking, combines the long-range, strategic, and psychological elements." "Mao's approach to preemption differed in the extraordinary attention he paid to psychological elements. His motivating force was less to inflict a decisive military first blow than to change the psychological balance, not so much to defeat the enemy as to alter his calculus of risks." "Having restored the psychological equation, in Chinese eyes, genuine deterrence has been achieved."

[342] See Wright ND (forthcoming) "The Neurobiology of Deterrence" for further discussion.

was the highly unexpected novel offer to speak in the Israeli Knesset that had a big psychological impact and opened the path to reconciliation.[343].

RECOMMENDATIONS

8.35.   Deterrence and escalation management are intimately related, neither alone is sufficient for the U.S. to cause intended and avoid unintended effects in the Grey Zone – and both should be considered together within the framework of *influence*.

8.36.   Both deterrence and escalation management have a fundamentally cognitive dimension.

> ➢ The "checklist for empathy" in Part I of this report provides one simple, operationalisable way to capture these, based in evidence.

8.37.   Controlling escalation involves not just minimising escalatory factors, but also positive accommodative and conciliatory gestures.

8.38.   Perceived fairness matters in shaping deals and deterrence (see Chapter 6).

8.39.   Culture should be taken seriously to understand key audiences. Understand potential adversaries' concepts of deterrence and escalation management. For example, Chinese deterrence concepts centre on managing a psychological balance and may involve pre-emption. The U.S. must anticipate such events within this deterrence paradigm.

---

[343] Christopher Roger Mitchell, *Gestures of Conciliation: Factors Contributing to Successful Olive Branches* (St. Martin's Press, 2000).

PART III CYBER IN THE GREY ZONE

Part III examines cyber in the Grey Zone. Chapter 9 asks if cyber presents particular challenges in the Grey Zone and, if so, what these mean for the U.S.. Chapter 10 looks specifically at Chinese and Russian cyber Grey Zone activities against audiences outside their borders at both the state and population levels. Given the difficulty in identifying Russian and Chinese external activities using only information from the public domain, we also describe their domestic cyber security activities.

Chapter 9: Cognitive Factors in Grey Zone Cyber

With Stefanie Hills (Loughborough University, UK)

9.1.   Cyber activity presents specific challenges in the Grey Zone:

> ➢ Technology changes, but the humans on the receiving end of influence remain human. The aim is to influence human psychology, so cognitive factors provide a solid bedrock for anticipating cyber effects.
> ➢ New technologies provide opportunities for potential adversaries to leapfrog U.S. cyber capabilities and to pursue highly asymmetric strategies.
> ➢ "Chemically pure ambiguity": The difficulty of attributing cyber actions magnifies the challenge of ambiguity in cyber.
> ➢ Greater difficulty defining the Grey Zone's lower and upper boundaries in cyber increase the potential for escalation.
> ➢ The unexpected nature of cyber activities to those on the receiving end may render them more escalatory than is understood by those making the actions.

9.2.   This chapter first looks at the characteristics of cyber in the grey zone. It then discusses ambiguity, fairness and legitimacy, norms and deterrence and escalation management.

CYBER IN THE GREY ZONE

9.3.   While technology changes the character of influence operations, the humans on the receiving end remain human. Understanding human motivation and decision-making thus provides a solid bedrock for anticipating effects. However, cyber clearly changes the character of influence capabilities and strategies.

9.4.   New information and communication technologies present new threats and opportunities for the U.S. and its potential adversaries. Notably, they enable adversaries to potentially "leapfrog" U.S. capabilities in these new technologies, greatly facilitate penetration across geographical boundaries and provide powerful asymmetric tools to sidestep overwhelming U.S. conventional military superiority. For example, just as Improvised Explosive Devices cost adversaries only a few dollars but imposed huge, asymmetric costs on Coalition forces in Iraq post-2003, so too can

adversaries compete asymmetrically in the information space. Daesh can produce high quality, fast, highly effective products that impact on target audiences in the region and Western countries.

Cyber and the boundaries of Grey Zone activity

9.5. Cyber presents particular challenges for considering what makes activity "Grey Zone" rather than "normal competition" or war (Fig. 9.1). For example, "normal competition" between states would be considered to include an element of data collection on other states' capabilities and intentions.

9.6. One may consider that cyber actions cross the "lower bound" of the Grey Zone from "normal competition" to Gray Zone activity when they are either: (a) sufficiently large in and of themselves (e.g. to threaten regime legitimacy within the target state); (b) when they are perpetrated with high enough frequency that their cumulative effect is sufficiently large (e.g. cyber espionage falls into the Gray Zone where it is perpetrated excessively and persistently; or persistent economic activity[344]); or (c) when conducted in concert with non-cyber actions such that together their cumulative effect is sufficiently large.

		Total war	
		Limited war	
		WAR	
Crises	Many smaller actions	Single/few large actions	**GREY ZONE**
Crises	"Normal" competition (e.g. economic competition, espionage)		**PEACE**

Figure 9.1: Cyber in the grey zone

9.7. The 'upper bound' of what makes cyber actions cross from the Grey Zone into war is unclear. Indeed, some scholars argue that there will be no cyber war, in the sense that no 'pure' cyber act can be an act of war.[345] We would argue that only a most extreme pure cyber action (e.g. one that significantly compromised the nuclear 'second strike' capability) or a significant cyber action following a prolonged conventional escalation scenario (e.g. a significant compromise of U.S. conventional "use-it-or-lose-it" early warning capabilities in China-U.S. escalation scenario) could

---

[344] An analogy is stalking or anti-social behaivour, where each individual act may not be problematic, but their cumulative effect constitutes a crime.

[345] Thomas Rid, *Cyber War Will Not Take Place*, 1 edition (Oxford ; New York: Oxford University Press, 2013). Rid argues that p. xiv. "cyber war has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future" and that. "All past and present cyber attacks are "sophisticated versions of three activities…as old as human conflict itself: sabotage, espionage, and subversion" This is because a purely cyber action has not fulfiled the first of three characteristics he uses to define war, pp. 1-2 "War is violent", "War is instrumental" and "An act of war is always political"

by itself cross the boundary to war. However, cyber actions may significantly contribute to escalation scenarios leading to war.

Different international concepts of cyber conflict

9.8.   Grey Zone activities necessarily involve both the U.S. and potential adversaries; and thus, it is crucial to understand how the U.S. and adversaries conceptualize cyber and information operations.

9.9.   The Joint US Military definition for 'Cyber Warfare' is "an armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyberattack, cyber defense, and cyber enabling actions." [346] China's People's Liberation Army (PLA), meanwhile, uses the term only to describe the Western understanding of cyber conflict as something that is restricted to the cyber domain as opposed to encompassing other areas of the "information space".[347]

9.10.   Russia and China more commonly use the term "Information Warfare", a term that used to also be used by the West but has largely been retired in favour of explicitly distinguishing between disciplines such as psychological operations, influence operations, and strategic communications[348].

9.11.   Arquilla and Ronfeldt (1993) described Information Warfare as "the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries."[349]

9.12.   The Chinese understanding of Information Warfare was initially based on western concepts, but has increasingly moved towards evolving its own orientation[350]. Chinese experts believe that the essence of Information Warfare is "the sum of information capabilities capable of breaking the will to resist by attacking an enemy's cognitive understanding and convictions, forcing it to give up all resistance and terminate the war".[351]

9.13.   In 1999 Xie Guang (Chinese Vice Minister of Science and Technology and Industry for National Defence at the time), defined Information Warfare as follows:

"Information Warfare in military sense means overall use of various types (of) information technologies, equipment and systems, particularly his command systems, to shake determination of enemy's policy makers and at the same time, the use of all the means possible to ensure that that one's own systems are not damaged or disturbed."[352]

---

[346] Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English" (5th International Conference on Cyber Conflict, Talinn: NATO CCD COE Publications, 2013).
[347] Ibid.
[348] Ibid.
[349] J. Arquilla and D. Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (1993): 141–60.
[350] Giles and Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English."
[351] Vinod Anand, "Chinese Concepts and Capabilities of Information Warfare.," *Strategic Analysis, Indian Institute for Defence Studies and Analyses* 30, no. 4 (2006), http://www.idsa.in/strategicanalysis/ChineseConceptsandCapabilitiesofInformationWarfare_vanand_1006.
[352] Ibid.

AUDIENCE, MESSAGES AND MESSENGERS IN THE CYBER DOMAIN

9.14.   The principles of influence in cyber are those examined in Part I—which considered them according to audience, messages and messenger—although as with any domain the character of influence is particular to cyber.

9.15.   **Audience** analysis is affected by the character of cyber in multiple ways. One may often be able to acquire more detailed information about individuals and target populations (e.g. commercial microtargeting); although in other cases linking real-world individuals to online personas may be more difficult. Whether or not target populations can access or be accessed via cyber varies widely within countries (e.g. by age group in developed countries) and between countries (e.g. big digital divides in access exist). For instance, some populations, such as in China, have a high numbers of smartphone users, whilst smartphone penetration in other states and regions is still relatively minimal. Ambiguity remains a significant factor and at state level it must be considered whether the message recipient has the capacity to understand the message sent through a particular cyber action.

9.16.   Cyber **messages:** in contrast to conventional messages can benefit from better audience analysis and can subsequently be more specific and tailored to the target audience.

9.17.   Cyber **messengers:** One must consider reach, language and ambiguity. Anticipating reach and language in cyber requires considering the popularity of different communication channels and social media platforms. China for example has its own domestic platforms, such as the microblogging service Weibo, and heavily restricts access to global social media networks. Cyber relies on relatively new technologies that can make attribution extremely difficult – and the resulting ambiguity is discussed next.

Box 9.1: The United States as a Cyber Target

The Government Accountability Office (GAO) reports that **between 2006 and 2015, the number of cyberattacks climbed 1,300 percent** — from 5,500 to over 77,000 a year at 24 federal agencies.[353]

In 2015, Russian hackers attacked the State Department email system in what was called the "worst ever" cyberattack against a federal agency. Also in 2015, the U.S. Office of Personnel Management reported 5.6 million Americans' fingerprints were stolen in a malicious cyberattack.

In March 2016, Chinese government hackers continued a malicious pattern of cyber attacks on U.S. government and private networks, according to U.S. Cyber Command chief Mike Rogers. China has been linked by U.S. intelligence agencies to wide-ranging cyber attacks aimed at stealing information and mapping critical computer networks for future attacks in a crisis or conflict.

---

[353] Government Accountability Office, "Information Security - Agencies Need toImprove Controls over Selected High-Impact Systems," Report to Congressional Requesters, (2016), http://www.gao.gov/assets/680/677293.pdf.

"CHEMICALLY PURE AMBIGUITY" IN THE CYBER GREY ZONE

9.18.   Ambiguity and problems of attribution are central to cyber activities. It is not only difficult for Governments to establish unambiguous versions of events (e.g. a DPRK or Russian source of a cyber action that may justify retaliation) but also to communicate that version of events unambiguously to key local and allied audiences.

9.19.   Martin Libicki of Rand describes cyberspace as 'tailor-made for ambiguity' and outlines several different ambiguities in the cyberwarfare domain.[354] The effects of a cyber-attack are often invisible to the outside world and attribution is frequently unclear. Even in cases where attribution can be determined, the purpose of the activity or attack may still be obscure. Cyberattacks used in lieu of kinetic methods create greater ambiguity in terms of effects, sources, and motives. Effective cyberattacks change the risk profile of certain actions, usually making them more attractive. Cyberattacks can create uncertainty when utilized by one state with the aim of affecting the outcome in another, without visible or even implied commitment. Cyberattacks provide victims with the option to deny an attack even took place in order to avoid admitting vulnerability, as being hacked generally indicates inadequate security measures.[355]

9.20.   Similar issues of ambiguity are raised by Antonia Chayes, who states that cyberattacks and cyberwarfare raise issues of self-protection, the ability to fend off or deny an attack, attribution about the origin of attack, and effectiveness of response[356]. She notes difficulties regarding identifying precisely when an attack or intrusion has taken place, whom it was perpetrated by, whether more than an internal repair and protect response is appropriate, and if so what type of response is deemed legal and proportionate. Factual uncertainty about the source of a cyberattack effectively guarantees legal uncertainty under international as well as domestic law. A lot of uncertainty lies in differentiating between normal levels of (predominantly economic) espionage committed by state actors, and hostile, line-crossing pre-cursors to cyberattack as well as in the difficulties to clarify at which point a cyberattack constitutes a military attack.[357]

9.21.   Private ownership of critical infrastructure and the blurring of civilian and military involvement provide an additional source of ambiguity. Matthew Crosston explores these issues, noting that international laws on conventional conflict are able to differentiate between civilian and military sectors, but there is a significant civilian/military ambiguity in the cyber domain that makes target differentiation unlikely or even impossible.[358] This is the key issue interfering with the creation of rules surrounding cyber conduct and cyber war behaviour. Most military networks that would initiate and enact a cyber-attack depend upon and work within countless civilian networks. Many of the actors that are part of the planning, initiation, and

---

[354] Martin Libicki, "The Strategic Use of Ambiguity in Cyberspace," *Military and Strategic Affairs* 3, no. 3 (2011).
[355] Ibid.
[356] Antonia Chayes, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6 (2015): 474–519.
[357] Ibid.
[358] Matthew Crosston, "DUQU's Dilemma: The Ambiguity Assertion and the Futility of Sanitized Cyber War," in *Leading Issues in Cyber Warfare and Security: Cyber Warfare and Security*, ed. J. Ryan, vol. 2 (Reading: ACPIL, 2015).

deployment of cyber-attacks are not necessarily formal military but civilian employees of government agencies, government contractors, or proxies acting on behalf of governments.

9.22.   The ambiguity problem is thus not limited to the problem of figuring out attribution but also extends to the inherent and purposeful ambiguity that lies in the critical infrastructure used to house, develop, and utilise a state's cyber capabilities. The inability to establish the military/civilian separation means that lethality could be greater by reaching more than just military casualties and damage could extend beyond military facilities.

Box 9.2: Stuxnet

Developed allegedly as a joint US-Israeli project in the mid-2000s, the Stuxnet worm was unleashed unto the Iranian Natanz nuclear facility in 2009 – most likely through an infected USB stick. Stuxnet specifically targeted programmable logic controllers (PLCs), which allow the automation of electromechanical processes.

In a December 2010 report the Institute for Science and National Security suggested that Stuxnet was likely responsible for the destruction of up to 1,000 centrifuges between November 2009 and January 2010, concluding that

"The attacks seem designed to force a change in the centrifuge's rotor speed, first raising the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge. If its goal was to quickly destroy all the centrifuges in the FEP [Fuel Enrichment Plant], Stuxnet failed. But if the goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating the FEP, while making detection difficult, it may have succeeded, at least temporarily."[359]

The report further notes that Iranian authorities have attempted to conceal the breakdown by installing new centrifuges on a large scale.

DETERRENCE AND ESCALATION MANAGEMENT

9.23.   Like all other deterrence, cyber deterrence succeeds when an adversary decides not to act. Such a decision follows the audience's assessment: Do the costs of cyber action outweigh its benefits and do the benefits of restraint in cyberspace outweigh its cost.[360]

---

[359] David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" (Washington, D.C: Institute for Science and International Security, 2010), http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf.
[360] Martin Libicki, "Cyberdeterrence and Cyberwar" (RAND Corporation, 2009).

9.24.   According to Lupovici (2011) cyber deterrence can work under certain circumstances, but problems associated with the defender's capabilities, the defender's willingness to use them, and the defender's ability to convey a message of deterrence to a potential enemy greatly limits the possibility of successful deterrence.[361] Lupovici outlines the difficulties of deterrence in cyberwarfare in terms of capability, credibility, and conveying the threat.

9.25.   Cyberwarfare allows weaker players to move confrontation into an environment in which they can maximise profits whilst risking relatively little. The more technologically developed an actor is, the more susceptible they are to cyberattacks. The possibility of retaliation is vastly reduced against weaker players and any credible threat of deterrence is lessened, especially when attacks are led by individuals and other non-state actors who do not own information systems that could be threatened with damage.

9.26.   Cyberwarfare entry costs are usually lower for the weaker side, which increases difficulties in presenting and executing the deterrent threat required in order to prevent such action. Additionally, domestic and international public opinion may limit the credibility of threat of retaliation due to the nature of cyberwarfare and the difficulties relating to the attribution of attacks.

9.27.   Problems relating to conveying the threat of retaliation to potential challengers lie for example in their diverse nature. The source of an attack may be another state entity or organization, but could also be a single individual or rogue group acting from within the targeted state itself or elsewhere.

9.28.   Deterrence requires the potential challenger to be aware of the defender's capabilities and willingness to use them ahead of time. It is difficult enough to identify the source of the damage even after the attack, it is near impossible to do so in advance. Deterrence is most effective when the threat – even inexplicitly – is aimed at specific actors rather than an undifferentiated audience of potential challengers.

9.29.   Lupovici does, however, identify some opportunities for deterrence in cyberwarfare in specific circumstances. He sees one option in the threat of asymmetric retaliation not limited to cyberspace[362]. In the case of a state threatening to act by means of cyberwarfare, the deterrent threat towards it may be based on the broadest range of capabilities the defending nation has at its disposal. These threats could be economic or military in nature. Threats posed by individuals and non-state actors could be deterred by employing threats of domestic or international judicial response as well as traditional military action. This can tip the balance from superiority of the challenger in the cyberspace sphere to their inferiority in other domains.

9.30.   Morgan (2010) suggests serial deterrence as useful in confronting cyberwarfare threats, stating that cyberattacks are highly likely to be manageable primarily through applications of repeated harmful responses over an extended period.[363]

9.31.   Both Lupovici and Morgan identify a further issue in the exposure of the capabilities of the defender. Whilst this problem is inherent in every form of deterrence in cyberspace, he deems it particularly acute serial-deterrence over longer period of

---

[361] Amir Lupovici, "Cyber Warfare and Deterrence," *Military and Strategic Affairs* 3, no. 3 (2011).
[362] Ibid.
[363] Patrick Morgan, *Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm* (National Academies Press, 2010).

time. Exposing the offensive capabilities as the consequence of repeated attack could serve as a basis of knowledge or inspiration for the challenger.

Escalation management

9.32.   Libicki (2012) states that success of escalation management depends on the fact that both sides would prefer less disruption and violence rather than more, albeit necessarily before they've made their point to each other.[364] He refers to escalation in cyberspace as 'a speculative topic', asserting that we lack a discrete metric for cyberwar and thus have no way to measure the proportionality of cyberattacks in a systematic and consistent manner. Controlling cyber-escalation is important because matters may not end in cyberspace.

9.33.   Libicki summarises the motives for escalation as follows:

> ➢ Gain military advantage: Military advantage from escalation must trump whatever military disadvantage arises when the opponent does the same) – calculating net advantage is difficult.
>
> ➢ Signal seriousness (to one's own side as well as to the other): To one's own side it's a signal of support, to the other side escalation may convey that a boundary has been overstepped, or that the outcome of a particular conflict is highly significant (where cyber-escalation is supporting an existing military operation).
>
> ➢ Demonstrate power: "We can do this to your systems despite your best efforts to keep us out". Contest of risk-taking (see Schelling's Arms and Influence). Presumption of 'escalation dominance' – the ability to outcompete one's enemy at all levels of escalation.
>
> ➢ Test the temper of opponents: How far are they willing to go? Are they rational and measured or irrational and erratic? Escalatory moves to gauge a reaction.

9.34.   According to Libicki, escalation (just like deterrence) only works if the adversary believes it does. The adversary's perception of red lines determines whether one's own cyberattacks are escalatory.

9.35.   Disrupting problematic communication outlets (may be viewed as a step in favour of crisis resolution, but might also be viewed as a violation of sovereignty). Cyberattacks may be used by victims of small-scale aggression to indicate displeasure whilst keeping the risk of escalation at bay.

9.36.   Rattray and Healey (2010) argue that even deterrence that is unsuccessful in completely preventing an attack, can ultimately still serve as a means of escalation control by serving to limit the escalation in scope or lethality.[365]

9.37.   Successful escalation control could mean that each adversary of a conflict might choose to limit themselves to only non-kinetic operations for a number of reasons, but perhaps the most compelling would be that neither adversary would be willing to

---

[364] Martin Libicki, "Crisis and Escalation in Cyberwar" (RAND Corporation, 2012).

[365] Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 2010.

escalate from cyber force to kinetic. Even if the effects of the cyber conflict were equivalent to those from a kinetic armed attack (in terms of lethality and significant property destruction), escalation to kinetic operations could entail possibly unacceptable risks to both sides—from international condemnation for initiating kinetic activity, or uncertainty relating to how the other side might further escalate.

Box 9.3: Advanced Persistent Threat

An advanced persistent threat (APT) is a highly covert long-term a set of continuous computer hacking processes targeting a specific entity. APTs are used to target either private organizations, states or both for economic or political motives. Sophisticated and severely complicated malware, such as Stuxnet, DUQU, and Red October have all successfully evaded detection for a significant period of time, in some cases for several years.[366] APTs tend to require significant technical and financial resources which indicates that attackers are generally well organised and likely to be working under a state umbrella.[367] APTs are used to pursue a variety of aims. Whilst Stuxnet's primary aim was sabotage, DUQU's and Red October's objective was espionage[368]. Red October was discovered in 2012, but is believed to have been active since 2007, targeting diplomatic, governmental and scientific institutions by disseminating malicious MS Word and Excel documents which exploited known vulnerabilities[369]. Each institution was targeted with tailor-made malware and email messages designed to increase the probability of the file being opened by the victim.[370]

NORMS FOR CYBER CONFLICT – CREATION AND CHANGE

9.38. The creation of "norms" (i.e. "rules of the road" that actors expect) for cyber actions are important but presents a formidable challenge. Norms are a good idea because all actors face the challenge that complex information systems are very hard to defend; because deterrence is difficult due to "chemically pure ambiguity" regarding who conducted an attack or if it even took place; and where verification of formal arms limitation treaties would be difficult. However, norms are hard to create now partly because of the same reasons why they are useful (e.g. attribution and verification), as well as because norms' effectiveness require at least tacit agreement between potentially antagonistic actors (e.g. Western nations, Russia and China)

---

[366] Nikos Virvilis and Dimitris Gritzalis, "The Big Four - What We Did Wrong in Advanced Persistent Threat Detection" (IEEE International Conference on Availability, Reliability and Security, CPS, 2013), 248–54.
[367] Ibid.
[368] B. Bencsath et al., "The Cousins of Stuxnet: Duqu, Flame, and Gauss.," *Future Internet* 4, no. 4 (2012): 971–1003.
[369] Kapersky Labs, "'Red October' Diplomatic Cyber Attacks Investigation - Securelist," accessed March 31, 2017, https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/.
[370] Virvilis and Gritzalis, "The Big Four - What We Did Wrong in Advanced Persistent Threat Detection."

with different concepts about cyber[371] and some have highly active domestic security programmes.

9.39.   The pursuit of international agreement to limit cyber conflict dates back to the 1990s. This was initially pursued through focusing on treaties as a means of promoting security and stability. Lewis (2011) described these treaty drafts as 'unimplementable', stating that "binding commitments to avoid attack or hostile actions may be unworkable, if only because potential opponents are unlikely to observe them."[372] An ever-increasing recognition that there is a need for agreements to regulate cyber behaviors at the international level remained, however, and the focus over time shifted from attempts to draft treaties to the proposing of cyber norms.

9.40.   In 2010, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security first recommended "dialogue among States to discuss norms pertaining to State use of ICTs [information and communications technology], to reduce collective risk and protect critical national and international infrastructure."[373]. Since then, various norm propositions have been made.

9.41.   Norm development is a challenge that in order to be effective must be pursued multilaterally, involving Western nations as well as in particular Russia, China, and Israel.

9.42.   Stevens (2012) suggests: "It may be that states can be persuaded to comply with international normative frameworks through a mix of inducement, coercion and moral pressure. So too might industry and civil society be persuaded to do their part through a gradual process of cultural learning, and all parties work together to achieve the "global culture of cyber security".[374]

9.43.   Some proposals rely heavily on comparing cyberspace, and associated security and deterrence issues, to other forms of governance debates. Hurwitz (2012) states that cyberspace, and thus the way to regulate it, is 'more like a social system based on a commons that can be sustained but also depleted', characterizing cyberspace as a shared resource[375].

Box 9.4: The Tallinn Manual (2013)[376] and Tallinn 2.0 (2017)[377]

Written between 2009 and 2012 at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence and originally entitled the 'Tallinn Manual on the

---

[371] Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in *Cyber Conflict (CyCon), 2013 5th International Conference on* (IEEE, 2013), 1–17, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6568390.

[372] James Lewis, "Confidence-Building and International Agreement in Cybersecurity," in *Confronting Cyber Conflict*, ed. Kerstin Vignard, Ross McCrae, and Jason Powers (Geneva: UNIDIR Disarmament Forum, 2011).

[373] United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

[374] Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy* 33, no. 1 (2012).

[375] Roger Hurwitz, "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterl* 6, no. 3 (2012): 21–22.

[376] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), http://csef.ru/media/articles/3990/3990.pdf.

[377] Michael N. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (New York, NY: Cambridge University Press, 2016).

International Law Applicable to Cyber Warfare', the Tallinn Manual is an academic and non-binding study on how international law (international humanitarian law and jus ad bellum) applies to cyber warfare and cyber conflict. Key norms addressed by the Tallinn Manual include:

> ➢ States may not knowingly allow cyber infrastructure located in their territory to be used for acts that adversely affect other States.
> ➢ States may be responsible for cyber operations directed against other States, even though those operations were not conducted by the security agencies. In particular, the state itself will be responsible under international law for any actions of individuals or groups who act under its direction. For instance, a State that calls on hacktivists to conduct cyber operations against other States will be responsible for those actions as if it had conducted them itself.
> ➢ The prohibition on the use of force in international law applies fully to cyber operations. Although international law has no well-defined threshold for determining when a cyber operation is a use of force, the Tallinn Manual states that any cyber operation that caused harm to individuals or damage to objects is qualified as a use of force.
> ➢ Cyber operations that merely cause inconvenience or irritation do not qualify as uses of force.

'Tallinn 2.0', the second edition of the Tallinn Manual was released in March 2017. Whilst the focus of the original Tallinn Manual rested on highly disruptive and destructive cyber-attacks and those taking place during armed conflict, which allowed for states to respond in self-defence, Tallinn 2.0 addresses malevolent cyber operations below this level, examining the international legal framework that applies to the grey areas of hostile cyber operations.[378]

LEGITIMACY AND JUSTICE

9.44. Whether cyber Grey Zone actions are perceived as legitimate will likely be determined in part by whether they are perceived as proportionate (which may be difficult if they are responses to others' cyber actions for which attribution is difficult) and whether they appropriately distinguish between military and civilian impacts (again potentially difficult with cyber actions). In addition to the legitimacy of actions, a broader issue related to legitimacy is that cyber actions may be seen as a threat to the legitimacy of a state to its domestic audience, for example where in Russia or China regime legitimacy is a primary concern and rests on extensive domestic cyber security apparatus. Below, we focus on the legitimacy of actions, for example for which various scholars argue in favor of more formal arrangements.

9.45. Ülgen (2016) states that in order to shape the regimes that govern cyberspace to the advantage of future generations, the United States and the European Union must

---

[378] Ibid.

work towards joint policy, arguing that there is a significant degree of convergence between the transatlantic partners and that these convergent areas should provide the basis for a new approach to creating a global cyber policy framework.[379] Ülgen proposes that the United States and European Union propose amendments to trade law in order to introduce penalties for economic cyberespionage, as well as to agree on a mandate for NATO to develop a more robust approach to cyberdeterrence. Ülgen also argues that the US and EU should lead efforts to codify norms governing the export of surveillance technologies in order to help constrain the capacity of illiberal regimes to restrict internet freedoms.

9.46. In relation to cyberwar in particular, Ülgen believes that cyberattacks must be defined to discriminate between civilian and military targets and comply with the proportionality principle, which is used to judge the lawfulness of an armed attack. New rules for containing cyberconflict also have to be devised to avoid unforeseen consequences of an attack. Ülgen argues that cyberweapons have unique capabilities of replication and dissemination, making it impossible for military planners to be aware of the scale and scope of destruction a cyberweapon may unleash in advance. This insecurity around collateral damage, Ülgen ascertains, is another argument for the creation of new rules for cyber conflict, akin to disarmament treaties in existence for conventional weaponry.

9.47. Marsden (2011) argues in favor of co-regulation, "offers the state a route back into questions of legitimacy, governance and human rights, thereby opening up more interesting conversations than a static no-regulation versus state regulation binary choice"[380].

9.48. Gervais (2012) ascertains that determining the active "theatre of conflict" is an integral aspect of evaluating cyber warfare's legal status. "If an attack occurs within the active theater of conflict, the law of armed conflict governs. But when a conventional attack occurs outside of the geographically limited theater of conflict, it is less clear how the laws of war apply."[381]. Gervais (2012) states that the challenge in defining the theatre of conflict in cyberspace is that any operation instantaneously involves internet infrastructure spread throughout multiple countries, but also argues that "fortunately, neither law nor custom supports confining a conflict to geographical boundaries", as conflicts that inherently cross borders are also common outside of the cyber realm.

Box 9.5: Economic cyber espionage, conflict and warfare

The term 'economic warfare' refers to an economic strategy based on the use of measures of which the primary effect is to weaken the economy of another state. Economic warfare can also more generally refer to a hostile relationship between two or more states in which one state tries to damage another's economy for economic, political or military purpose.[382]

---

[379] Sinan Ülgen, "Governing Cyberspace - A Road Map for Transatlantic Leadership" (Washington, DC.: Carnegie Endowment for International Peace, 2016).
[380] Christopher T. Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge, UK ; New York: Cambridge University Press, 2011).
[381] Michael Gervais, "Cyber Attacks and the Laws of War," *Berkeley Journal of International Law* 30, no. 2 (2012).
[382] R. T. Naylor, *Economic Warfare: Sanctions, Embargo Busting, and Their Human Cost* (Boston: Northeastern University Press, 2001).

Economic warfare is used as defensive means by countries to maintain their economic potential and diminish the economic potential of an enemy nation and its allies.[383] Economic warfare is conducted through various collective measures such as embargos or blockades, blacklisting, preclusive purchasing, capturing of enemy assets, economic espionage and boycotts. It is unclear when "normal" competition between states would cross into the grey zone, but high levels of cyber economic competition could do so.

An example of economic competition in the cyber domain would be China's excessive and persistent cyber espionage targeting both private companies as well as government departments (further detailed in Table 10.1 in the next chapter). This includes acts such as hacking into U.S. firms for the purpose of stealing trade and technology secrets in order to achieve a competitive advantage.[384] In 2015 US President Barack Obama and Chinese President Xi Jinping signed a bilateral Cyber Espionage agreement viewed cautiously as a positive first step to resolving tensions between the two states by a number of academics.[385]

In a 2014 report the U.S. Center for Strategic and International Studies estimated that global cost of cybercrime and espionage was $445 billion annually, with G20 nations suffering the bulk of the losses. The four largest economies in the world (the US, China, Japan, and Germany) are said to have lost $200 billion in 2013.[386] This is quite a conservative estimate compared to the $1 trillion quoted by President Obama.[387] In a 2016 Cybersecurity Ventures report, Steve Morgan states that the global cost of cybercrime and espionage has risen to $3 trillion in 2015 and is predicted to double again by 2021.[388] This figure includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. In a 2016 IBM security report the top five sectors facing the highest number of cyberattacks are healthcare, manufacturing, financial services, government, and transport.[389]

RECOMMENDATIONS

9.49. Western approaches must consider the human and societal—as much as the technological—aspects of cyber. This is more akin to the Chinese and Russian approaches.

9.50. Crucially, however, this does not mean the West should adopt the more offensive dimensions of Russian and Chinese approaches. Indeed, Western Governments

---

[383] Ibid.

[384] Andy Wong, "U.S. Turns Up Heat On Costly Commercial Cybertheft In China," *NPR.org*, 2013, http://www.npr.org/2013/05/07/181668369/u-s-turns-up-heat-on-costly-commercial-cyber-theft-in-china.

[385] Jacques deLisle and Jeffrey Vagle, "The Download on the U.S.-China Cyber Espionage Agreement," *Knowledge@Wharton*, 2015, http://knowledge.wharton.upenn.edu/article/the-download-on-the-u-s-china-cyber-espionage-agreement/.

[386] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," 2014.

[387] Ellen Nakashima and Andrea Peterson, "Cybercrime and Espionage Is Costing the Global Economy near Half a Trillion Dollars Annually," *Washington Post*, 2014, https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html.

[388] Steve Morgan, "Hackerpocalypse: A Cybercrime Revelation" (Cybersecurity Ventures, 2016).

[389] IBM Security, "X-Force Threat Intelligence Index 2017," 2016.

must try to build norms of cyber restraint that are perceived as legitimate. This more long-term goal must be pursued whilst also conducting short-term cyber contingencies: the *multiple timescales* that form one of the "Five Multiples of the Grey Zone."

9.51.   Restraint is even more imperative domestically, with extensive Russian and Chinese domestic cyber activities discussed in the next chapter.

Chapter 10: Russian and Chinese Cyber Approaches

With Oliver Fitton (University of Lancaster, UK) and

Stefanie Hills (Loughborough University, UK)

INTRODUCTION

10.1.   The overwhelming US dominance in conventional warfare forces revisionist states to employ asymmetric means in order to achieve political objectives – and cyber presents such an opportunity. How Russia and China seek to do this is shaped by:

> ➢ Russian and Chinese cyber policy appears to emphasize a different set of security challenges to its US and UK counterparts. Giles & Hagestad, for instance, argue that Russia and China do not subscribe to the euroatlantic consensus on "the nature and future of cyberspace" and have achieved commonalities in their understanding and use of related language: both states take a more cognitive and holistic socio-technical view of cyber- and information warfare and security; than the narrower euroatlantic understanding of the cyber domain.[390]
> ➢ Moreover, their domestic information operations significantly shape Russian and Chinese foreign information operations. Indeed, China in 2011 spent more on domestic security than on external security ($111 vs. $107 billion).[391]

10.2.   This chapter looks specifically at Chinese and Russian cyber Grey Zone activities against audiences outside their borders at both the state (Table 10.1) and population (Table 10.2) levels. Given the difficulty in identifying Russian and Chinese external activities using only information from the public domain, we also describe their domestic cyber security activities (Table 10.3).

RUSSIA: AUDIENCE, MESSAGE, MESSENGER

10.3.   First we ask how Russia thinks about Audiences, Messages, Messengers in their information/cyber operations abroad.

> #### *Audience*

10.4.   One of Russia's main target audiences for information operations is the Russian population of its near neighbors.[392] The ethnic Russian population just beyond Russia's western most boarders are considered by the Kremlin to be contested

---

[390] Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in *Cyber Conflict (CyCon), 2013 5th International Conference On* (IEEE, 2013), 1–17.
[391] Shambaugh, *China Goes Global.* p. 59
[392] Antonius JC Selhort, "Fear, Honor, Interest: An Analysis of Russia's Operations in the near Abroad (2007-2014)," (US Army Command and General Staff College, 2015), 48.

resources in a wider great power struggle between Russia and the West. [393] NATO has been particularly cognizant of the potential for conflict within ethnic Russian regions in Estonia, Latvia and Lithuania.[394] The mobilization of Russian populations in the near abroad is one of the key tasks of Russian information/cyber operations.

10.5.   Since 2008 justification for the Russian intervention in Eastern Europe (including the conflict in Georgia and Ukraine) has be founded upon the obligation of the Russian state to protect Russian 'citizenry' beyond its own boarders.[395] Alongside direct military support information/cyber operations have been employed in order to influence ethnic Russian populations and call them to action.

10.6.   In Georgia in 2008 a cyber operations campaign was waged alongside the kinetic intervention. This campaign included distributed denial of service attacks (DDoS) employed to sabotage government communication systems[396] alongside information/cyber operations such as website defacements. The website of the Georgian President was hacked and replaced with content comparing him to Hitler.[397]

10.7.   During the Ukraine conflict a pro-Russian hacking group carried out malware attacks[398] and sabotage operations against sites that were not towing the Russian narrative line.[399] These included website defacements and DDoS attacks in an attempt to secure an information monopoly for supportive social media and online news outlets such as Russia Today and Sputnik.[400]

Messengers

10.8.   Russian information operations take place mainly through Russian language television, radio and newspapers. These traditional news media are heavily influenced by the Kremlin as a result of Russian information security doctrine which emphasizes state control on national security grounded.[401]

10.9.   Influence is also achieved through the speeches, press releases and interviews given by political leaders. Information/cyber operations form a smaller subset of information campaigns carried out by Russia. Internet availability, rate of consumption of social media and relative direct influence over online media platforms each impact the utility

---

[393] Ibid., 47.

[394] For literature indicative of this interpretation see Janine Davidson, "Local Capacity Is the First Line of Defense against the Hybrid Threat," in *Transatlantic Security and Future of NATO Series* (Paris: The German Marshall Fund of the United States-Paris, 2015). And Michael O'Hanlon, "Nato after Crimea: How the Alliance Can Still Deter Russia," *Foreign Affairs* (2014), https://www.foreignaffairs.com/articles/baltics/2014-04-17/nato-after-crimea.

[395] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (2012): 8.

[396] Jose Nazario, "Politically Motivated Denial of Service Attacks," *The Virtual Battlefield: Perspectives on Cyber Warfare* (2009): 1.4.

[397] Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," 10.

[398] F-Secure Labs Security Response, "Blackenergy & Quedagh," (F-Secure, 2014), 2.

[399] Matthew J Schwartz, "Ddos Attacks Hit Nato, Ukraine Media Outlets," *InformationWeek: Dark Reading* (2014), http://www.darkreading.com/attacks-and-breaches/ddos-attacks-hit-nato-ukrainian-media-outlets/d/d-id/1127742.

[400] Russia Today and Sputnik are key elements of Russian Information warfare campaigns because of their connection to the Russian Regime and their social media following see Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," (Institute for the Study of War, 2015).

[401] Timothy Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," *Cyberpower and National Security* (2009).

of information/cyber operations.[402] Despite these restrictions social media and online news sources are still employed as tools of influence.

10.10.   Runet (The Russian Internet) consists of Russian language websites accessible by the wider online community. Runet is frequented by Russian language users inside and outside of The Russian Federation and forms a significant arena in which Russian information/cyber campaigns can take place. VK is the most popular social media platform in the Russian language and has been used extensively to influence Russian speaking populations.[403]

10.11.   The Russian government itself has embraced social media on Runet. The New York Times discovered VK "came under the control of businessmen allied with the Kremlin"[404] shortly before the invasion of Crimea. The Russian Federation is acutely aware of the power of social media even embracing western social media as a mouthpiece through which it can talk directly to its followers.[405]

10.12.   Social media and online news acts as a multiplier for the state influenced traditional media. The ability to record and distribute television presentation online through social media broadens the audience of those channels that would otherwise be constrained to the internal Russian populations. Replication also offers the opportunity to edit and distort broadcasts.

10.13.   The Kremlin is limited in its ability to push its agenda through globalized social media platforms because it has less control than it enjoys of Russian traditional media. However, the lack of control that the Russian state has over what is shared online beyond its borders is countered by the activities of independent and state supported online activists who absorb the Kremlin's message or create their own content which is sympathetic to it. CyberBerkut is perhaps the best example of this in recent years.[406]

10.14.   In addition to stealing and distributing sensitive information that furthers the Russian narrative CyberBerkut and other pro-Russian organisations are known to be using cyber operations, social engineering operations and information operations to monopolize the information space through denial of opponents' access to online services such as PayPal.[407]

Messages

10.15.   The element of information/cyber operations that differentiates them from cyber operations is the primacy of messages. There are two key repeated themes present in the Russian narrative:

---

[402] See Olesya Tkacheva et al., *Internet Freedom and Political Space* (Rand Corporation, 2013).

[403] Ibid., 141.

[404] Nickolay Kononov, "The Kremlin's Social Media Takeover," *The New York Times* (2014), http://www.nytimes.com/2014/03/11/opinion/the-kremlins-social-media-takeover.html?_r=0.

[405] The Russian Ministiry of Foreign Affairs can be found @mfa_russia on Twitter while the office of the President of the Russian Federation can be found @KremlinRussia_E

[406] Kiber Berkut, "Cyber - Berkut," http://www.cyber-berkut.ru/en/index.php.

[407] Tuomas Kerkkanen and Antti Kuronen, "Russia's Cyberwar in Ukraine Is Relentless – This Hacktivist Strikes Back," *Uutiset* (2016), http://yle.fi/uutiset/osasto/news/russias_cyberwar_in_ukraine_is_relentless__this_hacktivist_strikes_back/891820 0.

10.16. Nationalism is inherent within much of the material directed towards Russians located outside of The Russian Federation through state run or sympathetic channels. The idea of a single homogenous Russian state that usurps international borders is tied to sympathy for the revival of the golden age of the Soviet Union in which all Russian peoples are united under a single political banner.[408]

10.17. A subsection of this Cold war nostalgia is opposition to the United States and its influence. For example a unifying narrative is the interpretation that the failure of the Soviet Union in the Cold War was the result of US information warfare operations[409] an interpretation which influenced Russia's emerging focus upon hybrid operations.[410]

10.18. The second key narrative is Western hypocrisy or US imperialism. Such sentiments have been explicitly stated by Russian officials[411] and they have been taken to heart by many in the Russian population.[412] This sentiment is exhibited in information/cyber operations too with the production of content such as that created by Stop-Imperialism[413] and shared by Facebook pages such as Russia Truth.[414] This trend belies an underlying narrative of revisionism that is inherent to the concept of gray zone conflict.[415]

CHINA: AUDIENCE, MESSAGE, MESSENGER

10.19. Second, we ask how China thinks about Audiences, Messages, Messengers in their information/cyber operations abroad.

Audiences

10.20. Those actors who challenge Chinese "core interests" including "its territorial disputes, for example, over the islands in the South and East China Seas, Taiwan issues, China's political system, and foreign ships' military activities in its Exclusive Economic Zone" are the key audience for Chinese information/cyber operations.[416]

---

[408] Note that this is not necessarily on socialist grounds but rather nationalist glorification. Sergey Sukhankin and Alla Hurska, "Russian Informational and Propaganda Campaign against Ukraine Prior to the Euromaidan (2013-2014): Denying Sovereignty," *Securitologia* 21, no. 1 (2015): 36.

[409] See Thomas, "Nation-State Cyber Strategies: Examples from China and Russia."

[410] For example Valery Gerasimov, "Russian Military Doctrine," *Military-Industrial Kurier*, 27th February 2013. And analysis by Keir Giles, ""Information Troops"-a Russian Cyber Command?" (paper presented at the Cyber Conflict (ICCC), 2011 3rd International Conference on, 2011).

[411] See interview with Russian Security Council Secretary Nikolai Patrushev Elena Chernenko, "«За Дестабилизацией Украины Скрывается Попытка Радикального Ослабления России»," *Kommersant.ru* (2015), http://www.kommersant.ru/doc/2752250.

[412] These are older statistics but they demonstrate that in 2012 75% of Russians surveyed saw the US as an "aggressor which is trying to establish control over all the countries of the world." N Bondarenko et al., "Russian Public Opinion 2012-2013," (Moscow: Levada Analytical Center, 2013).

[413] See for example "Editor", "USA 1984: False Flags, Secret Prisons and Assassinations," *SI - Stop-Imperialism.com* (2015), http://stop-imperialism.com/2015/03/02/6521/.

[414] Russia Truth, "Facebook Group Page - Russia Truth," https://www.facebook.com/Russia-Truth-714016298647274/.

[415] Michael J Mazarr, "Mastering the Gray Zone: Understanding a Changing Era of Conflict," in *Advancing Strategic Thought Series* (United States Army War College, 2015), 10.

[416] Sangkuk Lee, "China's 'Three Warfares': Origins, Applications, and Organizations," *Journal of strategic studies* 37, no. 2 (2014): 198.

China targets the populations of its near neighbours and regional rivals with the objective to reinforce Chinese rights to regional hegemony.[417]

10.21. China's ability to influence regional rival's populations is restricted to some extent by the variety of languages in the South Asian region. Sympathetic groups of hacktivists may be only capable of targeting Mandarin speakers which is a particular problem when we consider that China's primary regional rival is Japan. This does not make influence operations impossible but it does mean that messages in, for example, Japanese and Thai are less likely to be perpetuated by casual Chinese Internet users.

Messengers

10.22. The Chinese are amongst the most prolific and blatant users of cyber operations in contravention of international laws and norms.[418] However access to the Internet is tightly controlled by the Chinese state with many social media platforms not easily accessible by the general public. YouTube, Facebook and Twitter are prime examples of giants of social media in the West that have been outlawed in China.

10.23. As a result the Chinese state has a strong grip on information operations that use computer systems to influence foreign populations because the average citizen is deterred from accessing common social media platforms used by those outside of the state. Operatives have to stick to social media platforms popular in Asia such as Weibo. For example a recent campaign that garnered support from Chinese celebrities was widely criticised for perpetuating the Chinese assertion of territory.[419]

10.24. The Internet is considered a risk to security and internal stability by the Chinese government. It is more likely therefore that Chinese information operations that target foreign populations will take place offline for example through cultural exchange program and bought newspaper articles.[420]

10.25. Here there is a nuance between information/cyber operations (typically subversive) and cyber operations (meaning sabotage and espionage). The Chinese are clearly content to use cyber sabotage and espionage but less comfortable with or able to launch cyber subversion operations.

Messages

10.26. The message present in extant Chinese information/cyber operations reflects that of more traditional information operations. Messages often allude to historical

---

[417] Laura Jackson's analysis of Chinese "media warfare" discusses target audiences for information operations in some detail: "Information at War: From China's Three Warfares to Nato's Narratives," in *Beyond Propaganda* (Legatum Institute, 2015), 7.

[418] In 2016 Symantec analysis puts China at the top of the league table for countries from which Botnets originate. Paul Wood et al., "Istr: Internet Security Threat Report," ed. Paul Wood (Symantec: Symantec, 2016), 60.

[419] Linh Tong, "The Social Media 'War' over the South China Sea," *The Diplomat* (2016), http://thediplomat.com/2016/07/the-social-media-war-over-the-south-china-sea/.

[420] "Information at War: From China's Three Warfares to Nato's Narratives," 7.

precedence for Chinese primacy over neighbours[421] or the creation of campaigns designed to spread messages of subversion that will influence adversaries.[422]

10.27. Once again in analysis of message we can see that China is less focused upon the creation distribution of ideas and more upon the control of the narrative space. Attacks on CNN in 2008 had a sabotage nature rather than one of counter narrative but the effect was to punish and silence a foreign critic.[423]

RUSSIAN AND CHINESE CYBER ACTIVITIES AT STATE AND POPULATION LEVEL

Table 10.1: Influencing other states: Comparing Russian and Chinese actions

Russia	China
Estonia In 2007 Estonia moved a Russian war memorial from central Tallinn to a military cemetery, outraging its Russian-speaking population and thereby leading to two days of riots. Whilst this was going on, the country's key websites (especially government and banking sites) were flooded with distributed denial-of-service (DDOS) attacks carried out by thousands of individual hijacked computers. This attack lasted several weeks and is attributed to state-sponsored Russian hackers.[424] Sweden Russia has recently been blamed for various cyberattacks on Sweden and is, according to the Swedish Head of Military Intelligence and the Security Service.[425] Russia was explicitly blamed for crashing Sweden's air traffic control in 2015.[426] Georgia 2008 combined kinetic and cyberattack, Distributed Denial of Service (DDoS) attacks on government websites, and an 'internet blockade'.[427] Ukraine	Chinese cyber activities have a strong focus on espionage. [429] Titan Rain In 2004, an analyst at Sandia National Laboratories traced the origins of an extensive cyber espionage ring back to a team of government sponsored researchers in Guangdong Province in China. The hackers, code named by the FBI 'Titan Rain', stole massive amounts of information from military labs, NASA, the World Bank, and others.[430] US State Department In 2006 China was blamed for a large-scale cyber break-in to the State Department's unclassified computer system, targeting its headquarters and offices dealing with China and North Korea, such as the Bureau of East Asian and Pacific Affairs. The bureau lost its Internet connectivity for several days.[431] GhostNet Following a 10-month investigation in 2009, Canadian researchers revealed a large cyber espionage ring they called 'GhostNet'. 'GhostNet' had allegedly penetrated more than 1,200 systems in 103 countries over the course

---

[421] "The Social Media 'War' over the South China Sea".

[422] Yvette Tan, "South China Sea: Chinese Social Media Urges Mango Boycott," *BBC NEws* (2016), http://www.bbc.co.uk/news/world-asia-china-36780967.

[423] Nazario, "Politically Motivated Denial of Service Attacks," 1.3.

[424] Libicki, "Cyberdeterrence and Cyberwar."

[425] "Russia Biggest Source of Cyberattacks on Sweden: Intelligence Head," December 12, 2016, https://www.thelocal.se/20161212/russia-biggest-source-of-cyberattacks-on-sweden-intelligence-head.

[426] Mary-Ann Russon, "Russia Blamed for Crashing Swedish Air Traffic Control to Test Electronic Warfare Capabilities," *International Business Times UK*, April 14, 2016, http://www.ibtimes.co.uk/russia-blamed-bringing-down-swedish-air-traffic-control-test-electronic-warfare-capabilities-1554895.

[427] David J. Smith, "Russian Cyber Strategy and the War Against Georgia," *Atlantic Council*, accessed March 31, 2017, http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia.

[429] Scott Harold, Martin C. Libicki, and Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace* (Santa Monica, California: RAND, 2016).

[430] Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," *Time*, 2005, http://content.time.com/time/magazine/article/0,9171,1098961,00.html.

[431] Christine Lagorio, "State Department Computers Hacked," *CBS/AP*, 2006, http://www.cbsnews.com/news/state-department-computers-hacked/.

Cyberattacks have been used in a broader strategy of information warfare. They encompass digital propaganda, denial-of-service (DoS) campaigns, website defacements, information leaks by hacktivist groups, and cyber espionage malware.[428]	of two years. The victims were foreign embassies, NGOs, news media institutions, foreign affairs ministries, and international organizations. Most notably, various Tibet-related organizations had been compromised, including the offices of the Dalai Lama. The attacks used Chinese malware and allegedly originated from Beijing.[432]

Table 10.2: Influencing foreign populations: comparing Russian and Chinese activity

Russia	China
<u>Web Brigades/Troll Armies</u> According to Hoskins and O'Laughlin (2015) and Gallagher (2015) the Kremlin employs hundreds of workers in state-sponsored 'troll factories' who post pro-Putin propaganda across news and social media forums. [433] <u>Russian English Language Media</u> English-language satellite channel Russia Today has been able to greatly extend its reach through video platforms like YouTube and associated Social Media sharing. Similarly, the Russia Today news website also has a considerable reach through Social Media sharing.	<u>Chinese Web Media</u> Hinck et al. (2016) found that Chinese foreign policy discourse primarily portrays China as a victim and responding to rather than initiating international provocation. China portrays itself as seeking a stable international environment and its economic and military rise as globally beneficial.[434] There is little evidence for Chinese cyber activity at foreign population-level, however, due to the nature of China's domestic population influence operations outlined in Table 10.2, some of their ongoing domestic activities are likely to regularly spill into the international sphere, especially through English language global social networks.

Table 10.3: Influencing their domestic populations: Russian and Chinese Cyber Activity

Russia	China
<u>Rossiya Segodnya</u> is a news agency wholly owned and operated by the Russian government, created in 2013 from the former RIA Novosti news service as well as the international radio service 'Voice of Russia'. <u>Doctrine of Information Security</u>: The Doctrine of Information Security declared the information sphere a "vital national asset that required state protection and policing" and used strong language	<u>Golden Shield Project</u> : Government run surveillance and censorship program that incorporates the 'Great Firewall of China', but also extends to keyword blocking, and the manual processing and removal of undesirable content.[435] <u>Silencing Collective Expression:</u> China does not necessarily disallow government criticism by individuals, but works hard to silence collective expression. Although criticism may shed a negative

---

[428] Kenneth Geers and NATO Cooperative Cyber Defence Centre of Excellence, *Cyber War in Perspective: Russian Aggression against Ukraine*, 2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf.

[432] Paul Simao, "Canadians Find Vast Computer Spy Network: Report," *Reuters*, March 28, 2009, http://www.reuters.com/article/us-security-spying-computers-idUSTRE52R2HQ20090328.

[433] Andrew Hoskins and Ben O'Loughlin, *War and Media: The Emergence of Diffused War* (Cambridge: Polity, 2010).

[434] Robert Hinck, Jacqelyn Manly, and Randolph Kluver, "Geopolitical Visions in Chinese Media," Report to PACOM Strategic Multilayer Analysis (Texas A&M University, 2016), http://nsiteam.com/social/wp-content/uploads/2017/01/Geopolitical-Visions-in-Chinese-media.pdf.

[435] Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review*, 2013, 1–18.

to assert the government's right to ensure ''the stability of the constitutional order, sovereignty, and the territorial integrity of Russian political, economic and social stability, the unconditional ensuring of legality, law and order, and the development of equal and mutually beneficial international cooperation.''. Deibert et al (2010) identify a further three types of controls. The first set of controls focus on denying access to specific Internet resources by directly blocking access to servers, domains, keywords, and IP addresses. The second set of controls seek to "create a legal and normative environment and technical capabilities that enable state actors to deny access to information resources as and when needed, while reducing the possibility of blowback or discovery". <u>Web Brigades</u> (Troll Armies) are state sponsored anonymous online political commentators that post pro-Putin propaganda across news sites, online forums, and social media. These are active domestically as well internationally.	light on policies and politicians, it is seen as unlikely to threaten their hold of power "as long as they manage to eliminate discussions associated with events that have collective action potential.[436] <u>50 Cent Party:</u> Domestically the purpose of state-sponsored internet commentators focusses on the purposeful distraction from debate and the derailing of social media discussions to suppress collective action. [437] <u>Fabricated Social Media Content:</u> King (2017) describes the phenomenon of "reverse censorship", whereby regime sponsored internet commentators post large numbers of fabricated social media comments, as if they were the genuine opinion of ordinary Chinese people.[438] <u>Public Opinion Warfare/Media Warfare:</u> Halper et al. (2013) identify similar media/public opinion warfare aims to Cheng (2012), which they summarize as: 1) Preserve friendly morale. 2) Generate public support at home and abroad. 3) Weaken an enemy's will to fight. 4) Alter an enemy's situational assessment.[439]

SELECTED BIBLIOGRAPHY

- Timothy Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," *Cyberpower and National Security* (2009).
- Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, California: Praeger, 2017).
- Jason R. Fritz, *China's Cyber Warfare: The Evolution of Strategic Doctrine* (Lanham, MD: Lexington Books, 2017).
- Nigel Inkster, *China's Cyber Power*, Adelphi 456 (Abingdon: Routledge, 2016).
- David C. Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival: Global Politics and Strategy* 56, no. 4 (2014): 7–22.
- Maria Snegovaya, "Russia Report 1: Putin's Information Warfare in Ukraine - Soviet Origins of Russian's Hybrid Warfare" (Institute for the Study of War, 2015)

---

[436] Ibid.
[437] Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument.," *American Political Science Review*, 2017.
[438] Ibid.
[439] Stefan Halper, "China: The Three Warfares" (University of Cambridge, 2013); Dean Cheng, "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response," *The Heritage Foundation*, 2012, http://www.heritage.org/research/reports/2012/11/winning-without-fighting-chinese-public-opinion-warfare-and-the-need-for-a-robust-american-response.

- ➤ Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (2012): 8.
- ➤ Scott Harold, Martin C. Libicki, and Astrid Stuth Cevallos, Getting to Yes with China in Cyberspace (Santa Monica, California: RAND, 2016).

PART IV MEASURING INFLUENCE IN THE GREY ZONE

Chapter 11: Measuring the Impact of Influence

11.1.   Measuring impact is necessary to understand effectiveness, improve influence activities and ensure accountability. It can be achieved without excessive administrative burden. Key points include:

  ➢ Planning and resourcing for evaluation is key. This needs to happen both before and after the intervention occurs. Evaluating multiple projects across contexts is necessary to answer key questions on impact, e.g. about contextual factors. Storing cases of success and failure is key for organisational learning. This presents security challenges.
  ➢ Rigour is the key concept in measuring impact, it is about being thorough and careful. Rigorous measurement can be qualitative (interviews, focus groups, observation) or quantitative (surveys, experiments).
  ➢ Behaviour change, perceptions or attitudes can all be the focus of measurement. Side effects such as in the target or other audiences, effect size, effect duration and context effects will also be important.
  ➢ Even if an intervention works, is it worth using? All interventions carry opportunity costs.
  ➢ Online behaviour presents specific challenges, for example in their relation to offline behaviours.

11.2.   This chapter will look at the importance of measuring influence, what to measure, measurement methods, and finally measuring influence online.

THE IMPORTANCE OF MEASURING INFLUENCE

11.3.   We must measure impact to improve influence activities, avoid adverse impacts and minimise opportunity costs. Evaluation is important for accountability, financially, legally and morally. However, business and government is often poor at evaluation and learning from evaluations over time. This is despite the availability of good, accessible guides to evaluation. There are three notable recent relevant examples: a Rand Corporation study on evaluating US Department of Defense Efforts to Inform,

Influence and Persuade[440], a NATO framework for evaluation of public diplomacy[441], and the Police What Works in Crime Reduction Tool Kit[442].

The centrality of useful rigour

11.4.   With the limited time, resources and data in the real world, the aim is to be sufficiently rigorous. Rigour is not necessarily synonymous with quantitative methods, as for many questions qualitative methods are most appropriate.

11.5.   Rigour helps to increase the reliability and validity of measurement, and to reduce bias. Rigour is being thorough and careful, which in measuring impact includes: the systematic approach to measurement design; an awareness of the importance of interpretation not perception or assumption; the systematic and thorough collection, analysis and interpretation of the data; maintaining detailed records of interviews and observations; using the Triangulation research method as a check on the validity of findings; the ability of an independent, trained investigator to re-analyse the data using the same processes and reach the same conclusions.[443] How rigorous one can be depends on resources and practical realities.

WHAT TO MEASURE?

11.6.   **General considerations:** It is good practice to specify beforehand what success and failure would look like, and to consider that stakeholders may have different views. Where possible, it is also good practice to report: pre-intervention and post-intervention data, and all outcomes indicated by the aims of the intervention. Overall, objectives should be SMART – specific, measurable, achievable, relevant and time-bound.[444]

11.7.   **Formative, process and summative measures**[445]**:** Formative evaluation is the pre-intervention research that helps shape the campaign. Process design documents the implementation of the process and thereby can be used to identify causes of failure. Summative evaluation seeks to determine outcomes that can be attributed to the intervention.

11.8.   **Behavioural change:** We most often want to change behaviour, either now or in the future.

11.9.   **Attitude or perception change:** We may not be able to measure behaviour, or we may wish to alter perceptions in order to create general behavioural change in the future (e.g. perceptions of the BBC or how far individuals identify with Daesh).

---

[440] Paul, C., Yeats, J. M., Clarke, C. P., Matthews, M., & Skrabala, L. (2015). Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Handbook for Practitioners. Rand Corporation.

[441] NATO, Joint Analysis and Lessons Learned Centre. (2013). *A Framework For The Strategic Planning & Evaluation Of Public Diplomacy.* Retrieved from http://www.jallc.nato.int/products/docs/A_Framework_for_the_Strategic_Planning_and_Evolution_of_Public_Diplomacy.pdf

[442] College of Policing - Crime Reduction Toolkit. Retrieved 2016, from http://whatworks.college.police.uk/toolkit/Pages/Toolkit.aspx

[443] Bowling, A. (1997) *Research Methods in Health.* Open University Press, Buckingham Philadelphia, p.121

[444] Paul et al., 2015

[445] Paul et al., 2015 p. 50

11.10. **Mechanism and process:** How do the intervention's activities cause change? This may be described as the "logic of the effort" or "theory of change". This may be investigated, e.g. using qualitative methods.

11.11. **Side effects:** Set out beforehand to measure important foreseeable side effects such as impact on a wider audience as discussed in chapter 2. Other side effects may be unanticipated, such as the adverse reaction of service personnel to increased transparency when receiving the anthrax vaccine (Box 15) and so will need to be looked for.

11.12. **Effect size:** How big are the impacts? An intervention may work very reliably, but the effect may not be sufficiently large to justify its use. Various metrics will be used in practice.

11.13. **Timing:** How long does the behavioural or perception change last? For example, will there be a need for a "top-up" intervention and, if so, can the same intervention be used or a different/modified influence activity needed? How rapidly does the impact occur? For example, early measurements may miss slower onset effects.

11.14. **Context:** Are there particular contexts or audiences that make an intervention more likely to work or not work? Is it generally applicable across all circumstances?

11.15. **Cost-effectiveness or resource-effectiveness:** This additional dimension may be needed in some situations. All activities carry opportunity costs. Cost-effectiveness of health interventions may be formally evaluated, for example, using the cost per Quality Adjusted Life Year, enabling bodies like the National Institute for Health and Care Excellence to compare cost-effectiveness of interventions. This may be feasible for some population level interventions (e.g. in the criminal justice system).

METHODS TO MEASURE THE IMPACT OF INFLUENCE

11.16. There are a variety of methods which can be used to measure the impact of influence. The following sections outline those methods. The choice of method will depend on a number of factors including the specific influence strategy, the target audience and factors available to measure.

Qualitative and Quantitative methods

11.17. Qualitative methods involve social research that does not rely on comparing quantities, for instance where quantitative surveys of populations do not permit detailed analysis of tastes or emotions, or of unknown unknowns. Methods include focus groups, ethnographies (direct observation of the activity of members of a particular social group), interviews or case studies. These methods are often useful for "how" or "why" questions. They are also useful for comparisons of small numbers of cases, such as nations or specific violent extremist groups. There is a challenge of generalisability—how far one case can explain other cases—and of reproducibility, and rigour is needed to avoid mere storytelling.[446]

11.18. Quantitative methods are the range of mathematical and statistical techniques used to analyse data. That is, they compare numbers.

---

[446] King, G., Keohane, RO., & Verba, S. (1994) *Designing Social Inquiry: Scientific Evidence in Qualitative Research*. Princeton University Press.

Convergent methods

11.19. Stronger conclusions can often be made by using multiple, complementary methods. Box 11.1 provides a good case involving the real-world study of an intervention to promote reconciliation in Rwanda. That study used the qualitative method of focus groups, the quantitative method of surveys to measure perceptions – and measured behaviour.

Box 11.1: Reconciliation in Rwanda[447]

Randomised controlled trials can be used to assess real world influence. A year-long field study was conducted with nearly 600 Rwandan citizens, prisoners, and genocide survivors who either listened to a soap opera about two communities struggling with prejudice and violence, or one on health. Data was collected using individual structured interviews and focus groups. In addition, behaviour was tested by recording group deliberations about how to share and supply batteries for the portable stereo and set of 14 cassette tapes of the radio program presented to each community at the end of the data collection. Given the monetary and entertainment value of a portable stereo, this discussion was of great significance to the participants. The measure captured spontaneous behaviour that participants believed to be "off the record". "Compared with a control group who listened to a health radio soap opera, listeners' perceptions of social norms and their behaviours changed with respect to intermarriage, open dissent, trust, empathy, cooperation, and trauma healing.

Measuring behavioural change

11.20. Measures often require clever acquisition, for example observing participants after an intervention when participants believe their behaviour is off the record, see box 11. Behavioural measures can also include, for example, financial, such as the reduction of Al Qaeda in Iraq's income from tax and extortion dropping from $12 million per month to a negligible level, or the degree to which an adversary is forced to respond. Official statistics such as crime rates or recidivism rates may also be used where appropriate.

Measuring attitudes and perceptions

11.21. Attitudes and perceptions can be identified using methods such as questionnaires. Caveats arise from the inconsistent relation of attitudes to behaviour, and well known biases in various sampling methods.[448]

Comparisons between intervention and control groups

---

[447] Paluck, E. L., & Green, D. P. (2009). Prejudice reduction: What works? A review and assessment of research and practice. *Annual review of psychology*, *60*, 339-367.
[448] Paul et al., 2015, Chapter 9

11.22. Comparisons between intervention and control groups can involve A/B testing, Randomised Controlled Trials or naturally-occurring experiments.

11.23. *AB testing:* This is a method often used in online marketing in which users are randomly exposed to variant A or B of a webpage or communication, and effectiveness is measured with desired metrics. Often multiple iterations and combinations are compared in series. The Obama 2012 Presidential re-election campaign used A/B testing to determine which messages generated most donations.[449] The Movember Foundation is a non-profit, global enterprise focused on raising awareness of men's health and fundraising. Movember tested two variants of their home page: the original one and a new one featuring a crowd of people. The homepage featuring the crowd outperformed the original one with 280, 000 more sign ups, 5 times more Facebook shares, 75% more email shares, and 28% more email donations[450]

11.24. *Randomised Controlled Trial:* These are similar to A/B testing but are more rigorously conducted and are not confined online. An example is the Rwanda case in Box 10.

11.25. *Naturally-occurring experiments*: For various administrative or other reasons, interventions are often only implemented in some areas, or are implemented differently in different areas. Although often not as well controlled as the preceding methods, these can provide valuable comparative data, particularly if planned in advance.

Measuring impact without a control group

11.26. In the real world when tackling issues like crime and national security it is often not possible for influence strategies to be deployed in only one region in order for comparison with a good comparator group. Routine statistics, such as crime or recidivism rates, can be helpful as baselines. This also highlights the importance of data collection and polling in potential target audiences ahead of time, e.g. conducted by the BBC, UK Government or others in areas at risk of political instability.

Measuring interventions against adaptive adversaries

11.27. Many important targets of influence cannot be evaluated in the more classical ways described above – and a key example is interventions against adversaries who learn and adapt. Consider the types of political reforms that were central to influence efforts and failures in Afghanistan and Iraq.[451] Success in such political reforms often rests on amassing political support, overcoming repeated cycles of reform and counter-reform with adaptive adversaries and involves highly interdependent political variables that are hard to separate. Specific recommendations for such cases are included below.

---

[449] Politics by numbers. (2016, March 26). *The Economist.* Retrieved from https://www.economist.com/special-report/2016/03/26/politics-by-numbers

[450] "A/B Testing Case Studies". Optimizely. Retrieved 2016-01-26 [Accessed 31 March 2016]

[451] Kleinfeld, R. (2015) *Improving Development Aid Design and Evaluation: Plan for Sailboats, Not Trains.* Washington, DC: Carnegie Endowment for International Peace

Multiple evaluations – beyond measuring one impact in one intervention

11.28. In the long-term it is critical that, where possible, key lessons and findings from an evaluation are available to other practitioners and contribute to the accumulation of knowledge from across multiple projects. This arises for four reasons:

11.29. First, it is useful to assess if findings can be replicated in multiple evaluations. A single success may be insufficient. There is currently an issue of replicability in psychology where around half of experiments in well controlled laboratory settings cannot be replicated[452] – a phenomenon affecting many scientific fields, such as cancer biology.[453] Critical to address this problem is to store and compare evaluations of multiple previous interventions—i.e. a repository, with due care taken for security of this highly sensitive data—which also facilitates organisational learning.

11.30. Second, test the intervention across contexts, as key contextual variables may render an intervention ineffective. See Box 11.2 on Israel-Palestine.

Box 11.2: Israel-Palestine[454]

A key lesson about common sense interventions is that their effectiveness may depend upon the conditions of the conflict. Take, for example, one of the most prevalent activities used in intergroup confidence building: 'perspective-taking' – asking someone to take the perspective of an individual member of another group in order to see the conflict through their eyes. Much previous experimental evidence illustrates that perspective-taking improves attitudes not only towards the target individual, but also the group they represent. However, in asymmetric conflicts the benefits of perspective-taking may be limited to members of only the relatively empowered group. In research conducted in the Middle East (with Israelis and Palestinians) a team from MIT found that a structured, online perspective-taking activity improved attitudes of Israelis towards Palestinians, but that the same exercise resulted in no change in attitudes among Palestinians towards Israelis. On the other hand, when Palestinians were instead given the opportunity to share their perspectives and be listened to by a member of the other group (what may be termed 'perspective-giving'), their attitudes towards Israelis changed dramatically, while perspective-giving had no effect on Israeli attitudes. Similar results were found in the very distinct asymmetric conflict in Arizona between White Americans and Mexican immigrants.

Although this study shows that the effectiveness of perspective-taking and perspective-giving depend upon a group's relative power, one would certainly not advocate employing purely asymmetric interventions. Rather, it suggests that an opening move may ask the disempowered group to give their perspective first, and structure the engagement such that the empowered group member is perceived to have actually heard what was said (e.g. summarize what their counterpart said without endorsing or denouncing) before

---

[452] Open Science Collaboration (2015) 'Estimating the Reproducibility of Psychological Science' in *Science* 349, no. 6251 (August 28, 2015): aac4716, doi:10.1126/science.aac4716.

[453] Begley, CG. and Ellis, LM. (2012) 'Drug Development: Raise Standards for Preclinical Cancer Research', in *Nature* 483, no. 7391 (March 29, 2012): pp.531–33, doi:10.1038/483531a.

[454] Bruneau, E. In Wright ND, Hewstone M, Lolliot S, Savage S, Ditlmann R, Bruneau E, Packer D, Castano E, Bock J (2015) *Helping the United States Security Coordinator for Israel and the Palestinian Authority understand the minds of others*, Report by the Carnegie Endowment for International Peace for the US DoD Joint Staff (122 pp.) USSC

> going on. Also, data from current dialogue programs show that Israelis spend much more time speaking than Palestinians. The study reported here suggests that programs should instead be structured so that they reverse this trend.

11.31. Third, common sense changes to the intervention may radically alter its effectiveness, so new versions of interventions should be evaluated again when possible. See Box 11.3 on Congo.

Box 11.3: Reconciliation in Congo[455]

In regions of intense conflict, like Rwanda immediately after the genocide and the Congo during their civil war, a radio soap opera that presents specific norms of intergroup reconciliation has been shown to cause measurable shifts in intergroup behaviours. Importantly, evaluation of the Congo intervention also revealed that adding another common-sense component to the soap opera intervention (a call-in talk show) completely nullified the positive effects of the soap opera.

11.32. Fourth, multiple influence strategies are often deployed simultaneously. Single evaluations struggle to tease apart multiple potential causal factors, which can be done by reviewing across multiple evaluations, for example by systematic review or meta-analysis.

RECOMMENDATIONS

11.33. Consider baseline measurements (e.g. polling) ahead of time, as often influence campaigns occur without comparator groups

11.34. Measure behavioural change where possible, as well as attitudes or perception. Try to specify these metrics and side effects before the campaign.

11.35. Some interventions require qualitative measurement and others quantitative. Try to combine methods where possible.

11.36. When facing adaptive adversaries design programs and funding to anticipate counter reforms and multiple battles. Key to this is ensuring flexibility for programmes and budgeting and testing hypotheses throughout a programme's life cycle.

11.37. Government should develop a clearinghouse of validated (and rejected) influence measures. This will give practitioners easy access to a database of measures tried and tested including both successes and failures.

---

[455] Paluck, E. L., & Green, D. P. (2009). Prejudice reduction: What works? A review and assessment of research and practice. *Annual review of psychology*, *60*, 339-367.

Appendix 1 Principles of influence in the Grey Zone: detailed evidence tables

We aim to summarise best practice for influence, based in empirical evidence, for two types of audience:

- **Populations:** Communication to communities, populations/subpopulations (e.g. encouraging the public's vigilance for threats, influencing a foreign population in counterinsurgency). This includes PsyOps/Military information support operations (MISO) and is analogous to mass health campaigns or mass marketing.
- **States:** e.g. how to negotiate, conduct deterrence operations, or manage escalation.

We did not separately examine the following types of audience: (a) Groups (e.g. Provisional IRA); (b) specific individuals (e.g. an individual of interest to the security services); or (c) online audiences as a separate category.

Methods: We examine multiple concepts. (1) Each concept was first identified through expert opinion. We particularly focus on aspects of influence relevant to both types of audience, as well as specific aspects of influence highly important to each type of audience. (2) Empirical evidence for/against each concept was identified using: experts and practitioners in behaviour change; experts from academia (including psychology, business, security studies and international relations) and industry; recent reports on behaviour change (e.g. the World Bank's 2015 report on Mind, Society and Behaviour) and books reviewing behaviour change; searches of academic databases and online resources; and grey literature produced by non-academic research or practitioner organisations or works cited by policy makers. We excluded evidence based on theoretical concepts rather than rigorously obtained empirical evidence. We used qualitative and quantitative evidence where appropriate (e.g. case studies for aspects of state interactions). Analyses were mainly conducted in 2016, with minor later additions.

Categories of evidence	Characteristics of the body of evidence
Strong	High quality body of evidence, large or medium in size, highly or moderately consistent, and contextually relevant.
Moderate	Moderate quality studies, medium size evidence body, moderate level of consistency. Studies may or may not be contextually relevant.
Low	Moderate-to-low quality studies, medium size evidence body, low levels of consistency. Studies may or may not be contextually relevant.
Nil	No/few studies exist.
Harmful	At least low evidence that the intervention is harmful.

The **strength of evidence** for each concept was rated as Strong, Moderate, Low, Nil or Harmful. Increased weight was given to convergent evidence (e.g. for the mass communication audience type, convergent evidence from diverse disciplines such as psychology, behavioural economics and marketing) and where it had been shown to matter in the real world (e.g. for the mass communication audience type, rigorous field studies not just laboratory experiments), and where the methods had been shown across cultures.

Three tables are included below—for the Chapter 2 Audiences, Chapter 3 Messages and Chapter 4 Messengers—and there is inevitably overlap between them. In each row is a concept from the report, and each column outlines evidence relating to each type of audience.

The tables form an appendix to the main report. We use evidence from our extensive interviews and other non-public expert sources throughout, but for reasons of space do not state this repeatedly. Also for reasons of space, we do not include here all the references included in the main text, and these tables below also focus on citing reviews and/or illustrative or important sources.

EVIDENCE FOR CHAPTER 2 - AUDIENCES

Concept	Communities and masses of individuals	State
Think "Outside-in" (Put yourself in the shoes of the audience) *[Paragraph 2.4 in the main text]*	STRONG *(a) That it is a challenge* Psychology of negotiation literature, largely lab experiments, e.g. (Bazerman et al. 2000). *(b) Improves performance* Lab experiments show improved negotiation with perspective taking traits and manipulations (Galinsky et al. 2008). (Waldron and Applegate 1998) analysed student conversations, in which those using tactics tailored to the target were rated more persuasive. With "standardised patients" in a medical student exam setting, (Blatt et al. 2010) showed receiving a perspective taking instruction versus neutral instruction increased patient satisfaction in three studies, across medical schools, clinical disciplines, and racially diverse students and "standardised patients" in the US. (Gass and Seiter 2013) book reviewing persuasion, p. 116 "This, to us, seems to be what persuasion is all about: adapting a message so it coincides with the receiver's frame of reference … called being market driven in business, "audience-centred" in in public speaking … may also be the most important lesson you can learn about how to be a successful persuader". Marketing/business literature shows firms commonly fail to think from the audience's perspective, and that being	STRONG Deterrence: Numerous reviews increasingly conclude deterrence must be tailored to each individual case based on a detailed understanding of the other side. E.g. (Freedman, 2004 pp. 58-59); (Quinlan 2004, p. 12) (Quinlan, 2004 p. 12); (Gray, 2003, p. ix, 9, 33); (Wheeler 2003, p. 76); (Payne 2001, pp. 422-3). Soft power: (Nye 2004) argues that Americans must listen. Note, however, there are dissenting views who argue that taking tailoring too far may result in less clear and thus effective messages, e.g. see (Knopf 2010, p. 9).

	more customer-focussed / market-orientated increases performance. This includes: Books with cases, e.g. (Gulati 2010), (Day and Moorman 2010), (Ellsworth 2002). Studies, e.g. (Morgan et al., 2009) show market orientation increased return on assets. Meta-analysis by (Kirca et al., 2005) shows increased market orientation increased performance.	
Structured guides for audience analysis in influence – there are many that are based in evidence, but with little evidence on the guides themselves in order to choose between them. *[Para 2.9]*	STRONG Literature review and interviews with academics and practitioners suggest little empirical comparison of the effectiveness of different structured frameworks or guides in terms of effectiveness at behaviour change outcomes. This includes for guides in health [e.g. the "Behavioural change wheel" (Michie et al., 2011), or NICE behaviour change guidelines]; the negotiation literature, e.g. (Malhotra and Bazerman 2012); broader behaviour change frameworks [e.g. MINDSPACE (Dolan et al. 2010) (Dolan et al., 2010; Messenger, Incentives, Norms, Defaults, Salience, Priming, Affect, Commitments, Ego) or EAST (Service et al. 2014) (Service et al., 2014, Easy, Attractive, Timely, Social)]; or remote personality profiling [e.g. revealed framework in (Taylor, Furnham, and Breeze 2014)] or direct application of structured professional judgment models to security. Overarching frameworks: (Darnton 2008) reviewed 60 models for HMG and produced an overarching framework for the use of multiple models or aspects of models as needed to understand important audience factors (Tables A1, A2 pp35-9.) Chatterton (2011) review of behaviour change for DECC also advocated a "multi-model" approach. Theory of planned behaviour has been evaluated with mixed results, e.g. (Sniehotta et al., 2014).	MODERATE Various structured approaches exist but with little public evidence on effectiveness.

	Models also include those used in marketing and Psychological operations / Military Information Support Operations, and Media (e.g. BBC Media Action) described in main text.	
Structured guides or frameworks: using a structured approach is better than not using one *[Para 2.10]*	MODERATE Literature review and interviews with academics and practitioners suggest little direct empirical evidence, but strong evidence from other fields. Evidence is mostly by analogy from other contexts, e.g. a guide for heart surgery in (Gigerenzer 2008); Surgical checklists (Gawande 2009) although note (Anthes 2015) for discussion of how implementation is important; flying and investment and other fields may be more successful with checklists but unclear evidence base (Gawande 2009). In addition, interviews with BBC Media Action highlighted organisational principles as a form of structured guide, e.g. the primary principle of being audience-centred.	MODERATE As for the Population level, the evidence is largely by analogy to other decision-making.
Self-interest/incentives (This is the use of incentives / disincentives; rewards / punishments; or gains / losses) *[checklist for empathy in Box 2.1 and Chapter 3]* *[Para 3.13]*	STRONG *(a) Use of incentives:* Lab: Experimental economics, e.g. Extensively covered in (Kagel and Roth 1995) and in (Camerer 2003) Crime: (Paternoster 2010) Extensive review shows "offenders and would-be offenders … certainly are rational in the sense that they respond to incentives and disincentives", e.g. the "risk of getting caught" and learn as expected with perceived after getting away with crime or being punished. Kamenica (2012) provides a review of how behavioural economics has shaped thinking about incentives. Madrian (2014) discusses uses of incentives informed by a behavioural approach in public policy making. STRONG *(b) Use of positive incentives* Gift giving works well, such as lobbyists in pharma (Steflox et al 1998).	STRONG *(a) Use of incentives:* Realist and liberal internationalist literature. MODERATE *(b) Use of positive incentives:* (Nincic 2010) (Spangler 1991) LOW *(c) Gain/loss asymmetries:* Prospect theory papers in International Relations: (Schaub 2004) (McDermott 2001) (Mercer 2005) (Haas 2001) (Stein and Pauly 1992) (Jervis 1992).

Health behaviour change by monetary incentives in a review by (Promberger and Marteau 2013)
(World Bank 2015) p.13 Nonmonetary gifts Small nonfinancial incentives and prizes—like lentils and metal dinner plates—were combined with a reliable immunization provider within the community in India. Among children aged 1–3, rates of full immunization were 39% with the lentils incentives compared to 18% in the group with only the reliable immunisation provision. In areas with no intervention, the rate of full immunisation was 6%.

MODERATE
(c) Gain/loss asymmetries:
Lab: (Kahneman and Tversky 1979; Tversky and Kahneman 1992).
Messaging: (Gallagher and Updegraff 2012) review of 94 studies comparing gain-framed to loss-framed messages, gain-framed messages consistently improved adoption of preventive behaviours (such as vaccinations) when compared to loss-framed messages with the same objective information.

STRONG
(d) Include hassle/transaction costs:
E.g. (Bettinger and others 2012) review 43 papers, appearing in 8 domains, showing that providing personalized assistance in completing the Free Application for Federal Student Aid (FAFSA) led to a 29 percent increase in two consecutive years of college enrolment among high school seniors in the program group of a randomized controlled trial, relative to the control group

STRONG
(e) Incentives' form can enhance effectiveness:
Enhance by unexpectedness or lotteries (Service et al. 2014) (Service, 2014). Balkans example of lottery.

	LOW *(f) Rebound effects/crowding out:* Chinese essay writing competitions amongst US POWs in Korean War would not pay them much, to avoid recoil at larger payments (Cialdini 2008, p80). Gneezy et al. study of Israeli day-care (although note dispute). Freedman (1965) showed that on male children moral arguments had longer term effects than threats. (Kohn 2000) reviews various literatures. However, no crowding out effect of incentives was reported for health behaviours in a review by (Promberger and Marteau 2013), although they note this may be due to the non-social nature of health and thus may be less applicable to security. *(g) Price rises lead to more sales* (Cialdini 2008) Arizona jewellery sales double when price is doubled.	
Fairness *[Checklist for empathy in Box 2.1 and Chapter 3]* *[Para 3.19]*	STRONG Extensive testing in the laboratory (Camerer 2003), across diverse cultures (Henrich et al. 2001) (e.g. Henrich et al) and with large stakes (e.g. Cameron, 2003). Bazerman et al (2000) negotiation literature. Tom Tyler's work shows extensive evidence for importance of procedural fairness in the US policing to maintain behavioural control. Scott Atran's work on sacred values e.g. (Berns et al. 2012). Moghaddam's work on fairness in the staircase to terrorism (Bongar, Brown, and Beutler 2006)	MODERATE Fairness in various aspects of international negotiation: (Knopf 2012) (Albin 2001) (Wang 2012) (Christensen 2015) Macroeconomics: (Akerlof and Shiller 2009) show effects of fairness.
Fear *[checklist for empathy in Box 3 and Chapter 3]* *[Para 3.16, 3.17]*	STRONG *(a) Fear matters:* Security Dilemma in ethnic conflict (Posen 1993) Terrorism (including strategic bombing) causes fear and behaviour change in target audiences, e.g. (Bongar, Brown, and Beutler 2006). However, this effect typically reduces over time and can be replaced by high	STRONG *(a) Fear matters:* E.g. Security Dilemma: (Jervis 2001; Booth and Wheeler 2007; Christensen 1999). STRONG *(b) What to do?* Transparency etc. (Steinberg and O`Hanlon, 2014)

	resilience and desire for retribution (Bongar, Brown, and Beutler 2006). MODERATE *(b) Fear appeal messages:* Meta-analysis, largely health, affecting attitudes, intentions and behaviours (Tannenbaum et al. 2015) concluded that (a) fear appeals are effective at positively influencing attitude, intentions, and behaviors. Other reviews stress that fear appeals can backfire if there are insufficiently plausible alternatives, e.g. (Cameron 2009), (Maloney, Lapinski, and Witte 2011), (Ruiter, Abraham, and Kok 2001), (Soames Job 1988)	
Identity	See below in Ch 2	
Status *[checklist for empathy in Box 2.1]*	STRONG *(a) Status matters:* For reviews, see e.g. Rosen (2005) on War and Human Nature; Frank (1985) on Human Behaviour and the Quest for Status; Frank (1999; 2005); Wright (1994) on evolutionary psychology; Loch et al. (2001) on status in organisations. (Munoz 2012) Status and Taliban in US MISO in Afghanistan. *(b) Use status to influence behaviour:* Reviewed by (World Bank 2015) p44, e.g.: (Larkin 2011) show salespeople in a U.S. company traded off approximately $30,000 in income to achieve membership in the firm's "club" for top performers. (Kosfeld and Neckermann 2011) show in a field experiment in Switzerland that individuals' performance improved by 12 percent on a one-time data entry task when they were told that the two people who put in the most effort would be rewarded with a congratulatory card and a personal thank-you from the managing director. (Ashraf, Bandiera, and Jack 2014) In a field experiment in Zambia, hairstylists and barbers recruited by a public	STRONG *(a) Status matters:* Status influences on state behaviour are suggested across diverse historical cases, with recent examinations including Russia and China (Larson and Shevchenko 2010), the 1850s Crimean conflict, Cold War etc. (Wohlforth 2009). (Shambaugh 2013) reviews Chinese foreign policy, arguing status accounts for key aspects of Chinese diplomatic behaviour, e.g. "face diplomacy" (Gries 2004). *(b) Use status to influence behaviour:* "Social creativity" has been suggested to manage competition over status, whereby different states achieve status in different fields (Larson and Shevchenko 2010; Wohlforth 2009).

	health organization to sell female condoms in their shops were randomly assigned to one of four groups: no rewards; a 90 percent margin on condom sales; a 10 percent margin on condom sales; or a nonfinancial reward in the form of stars stamped on a publicly displayed chart to represent each condom sale. After one year, hairdressers in the star treatment had sold twice as many condoms as hairdressers in any other group, on average. (Besley and Ghatak 2008) Status awards may be especially useful when the quality of individual outputs is difficult to measure precisely	
Expectations and unexpectedness *[checklist for empathy in Box 2.1]*	STRONG E.g. (Vosoughi, Roy, & Aral, 2018) Examined the spread of news online in a large social media study	STRONG Expectations and surprise in diplomatic and military confrontations, e.g. (Schelling 1966; Jervis 1976; Smoke 1977; Handel 1980; Handel 1981; Betts 1982)
Audience segmentation *[Para 2.19]*	STRONG Strong evidence relating to standard methods segmenting by e.g. age or geography, e.g. public health, marketing etc. (Gass and Seiter 2013) book review pp. 118-9, or (Kreuter and McClure 2004) for segmenting by cultural dimensions in health.	N/A
Audience data-driven division *[Para 2.19]*	STRONG (Miguéis, Camanho, and e Cunha 2012) supermarket personalisation. Amazon recommendation algorithms. Political campaigns such as Obama re-election 2012 (Economist, March 2016).	N/A
Audience division qualitative *[Para 2.19]*	STRONG E.g. Interviews with BBC Media Action, marketing experts and CVE experts. "Thick description" is also discussed by the (World Bank 2015) p. 194 and spotlight 4.	N/A
Unintended audiences *[Para 2.21]*	MODERATE Bell, 1984	MODERATE

	McKeganey (2005) on random drug testing in schoolchildren; Pyszczynsky et al. 2006 effect of mortality salience on US and Iranian students' attitudes.	Various authors note the importance of multiple audiences for signals and actions, e.g. in (Freedman 2004) p. 49 for deterrence.
Identity – shape narratives and decision-making *[Para 2.24]*	STRONG *(a) Identity matters:* HMG Foresight report (2013) Lab and field experiments, e.g. (Sherif et al. 1961; Bourdieu, 1977; Kleinman, 2006; Turner, 1985; Hoff et al., 2006; Hoff et al., 2014). STRONG *(b) Use in information operations:* (Munoz 2012) Western information operations did not much use nationalism and Pashtun identity, while Taliban did successfully.	STRONG *(a) Identity matters:* Nationalism as a driver of foreign policy, e.g. (Shambaugh 2013; Gries 2004; Fukuyama 2014). Identity more broadly as a driver of foreign policy, e.g. (Hopf 2002).
Identity – multiple overlapping identities [Para 2.25]	STRONG *(a) Existence of multiple overlapping identities.* Considerable lab and field evidence. WEAK *(b) Influence by focussing individuals on a specific identity:* Some semi-field experimental evidence: Priming UK football fan identities using questions about their clubs (Levine et al., 2005). Prisoners in Zurich maximum security jail primed with questionnaire on their prisoner identity were more dishonest in reporting coin tosses in experiment (Cohn et al., 2013). (Hoff and Pandey 2006; Hoff and Pandey 2014): High-caste and low-caste boys from villages in India were randomly assigned to groups that varied the salience of caste identity. When their caste was not revealed, high-caste and low-caste boys were statistically indistinguishable in solving mazes. Revealing caste in mixed classrooms decreased the performance of low-caste boys. But publicly revealing caste in caste-segregated classrooms—a marker of high-caste entitlement—depressed the performance of both high-caste and low-	WEAK Social creativity: (Wohlforth 2009b) (Larson and Shevchenko 2010b)

	caste boys, and again their performance was statistically indistinguishable. Historical case: Saving Bulgaria's Jews (Reicher et al., 2006).	
Identity – inadvertent effects [Para 2.26]	WEAK Flying while Muslim (Blackwood, Hopkins and Reicher (2015))	N/A
Attitudes [Para 2.28]	MODERATE *(a) Attitudes influence behaviour, but there is an important attitude-behaviour gap:* (Maio and Haddock 2009) MODERATE *(b) Attitudes follow behaviours:* (Maio and Haddock 2009) STRONG *(a) Attitudes influence behaviour, but there is an important attitude-behaviour gap:* (Maio and Haddock 2009) MODERATE *(d) Attitudes follow behaviours:* (Maio and Haddock 2009)	N/A
Age [Para 2.29]	STRONG *(a) Risk taking, aggression etc. differs by age* (Steinberg et al 2011; Steinberg 2004) LOW *(c) Influence susceptibility differs by age* (Hovland et al 1953)	LOW Limited work was found. E.g. (Horowitz, McDermott, & Stam, 2005) conduct an analysis.
Education level [2.31]	LOW Limited evidence relates the amount of education to responses to information in the West. For example, greater scientific literacy and numeracy in the US led to more extreme views on climate change – and as this occurred for both more individualist and more	N/A

	communitarian individuals, the more educated part of society was more polarised (Kahan et al. 2012). Found that UG educated servicemen and above were more persuaded by two-sided arguments, while those with less than UG education were more persuaded by one-sided arguments. Lumsdaine showed that two-sided is more effective in the face of counter-propaganda: Hovland, C. I., Lumsdaine, A. A., & Sheffield, F. D. (1949). The effects of presenting "one side" versus "both sides" in changing opinions on a controversial subject. Experiments on mass communication, Vol. 3. Studies in social psychology in World War II., (pp. 201-227). Princeton, NJ, US: Princeton University Press. State is covered by Lumsdaine, A. A., & Janis, I. L. (1953). Resistance to "counterpropaganda" produced by one-sided and two-sided "propaganda" presentations. Public Opinion Quarterly.	
Education type (e.g. engineers) [Para 2.31]	LOW Limited evidence relates the amount of education to how people respond to information in the West. Kahan et al. (2012), show greater scientific literacy and numeracy in the US led to more extreme views on climate change – and as this occurred for both more individualist and more communitarian individuals, the more educated parts of society became more polarised. Whether type of education affects susceptibility to influence is highly contested, as in disputed suggestions of engineers' susceptibility to violent extremism (Gambetta & Hertog, 2016).	N/A
Personality [Para 2.32]	LOW Some work suggests personality traits predict receptiveness to influence (Hirsh et al, 2012), for example, that extroverts are less susceptible to influence from authority figures (Alkis et al., 2015). However, it is unclear how reliable, important and practical such personality measures are for influencing behaviour.	N/A

Culture [Para 2.33]	STRONG	MODERATE
	Negotiation: Compared Salami slicing in US and Asian students (Petrova et al 2007). See also e.g. Bazerman et al. (2000) and DiMaggio (1997). Establishing culture's connection to the attitudes, values and established practices of targets of influence campaigns; understanding and engaging their common-sense or fundamental assumptions, e.g.: Mary Douglas' grid (constraint by rules) and group (desire for incorporation into a bounded group) typology identified four fundamental cultural orientations that co-exist and interact within and between communities: people (individuals, groups, networks, states) express their loyalties and moral principles, and their responsibilities to other members of their society - via a commitment to strong or weak group identities and strong or weak regulatory structures. She abstracts four 'figures' which have been extensively developed and applied to explain organizational structures and lines of influence, or blocks to influence. The four figures are: Isolates, Hierarchies, Individualists, Enclaves. (Mary Douglas 1970, *Natural symbols, explorations in cosmology*. Penguin) Motivation for group inclusion (Douglas as above). Loyalty to and/or rebellion against dominant values. Many studies note the importance of competing values, of acceptance and contestation of hierarchies of gender, age, class, etc. and acknowledge that communities are never homogeneous. (e.g. Gerd Bauman, *Contesting Culture*, 1996, Cambridge University Press, an ethnographic study of how young people in Southall, South London, identify with multiple and diverse cultural groupings). Others show how individuals can and do act against dominant values - often drawing on other common values in support of actions (e.g. Sophie Day *On the Game: Women and Sex Work* 2007 Pluto Press.	*(a) National culture* Cultural effects on negotiation at the state level is suggested by e.g., Solomon (1995) who looked at Chinese negotiations. Huntington (2002) argues for the importance of culture in world politics in the "Clash of civilisations". Cultures of nationalism are also supported by other academic perspectives, for example in the state supported conflation of culture and identity via public ritual, education systems, state symbols and the support of particular cultural values (e.g. Bruce Kapferer, *Legends of People, Myths of State*, Smithsonian Institution Press, 1988, a comparative study of nationalism in Australia and in Sri Lanka, drawing out the influence of nationalist thinking on war, racism and exclusion; John R. Bowen, *Why the French Don't Like Headscarves: Islam, the State, and Public Space*, 2008, Princeton University Press; Herzfeld, Michael. 2005. *Cultural intimacy: Social poetics in the nation-state.*, Routledge, shows how nation-states secure citizen loyalty by tolerating practices and attitudes that contradict official ideology; Verdery 1999 *The Political Lives of Dead Bodies: Reburial and Postsocialist Change*. Columbia University Press, argues that dead bodies are key sites for rethinking politics not as a series of technical and rational decisions or strategies among state citizens (liberal or not), but as a cultural politics of meaning, authority, and value-making that implicates whole worlds of contested spaces and times; Alessandro Zagato (ed) *The Event Of Charlie Hebdo: Imaginaries of Freedom and Control*, 2015 Berghahn Press; the volume analyses the influence the attacks have had in various spheres of social life, including the political, ideology, collective imaginaries, the media, and education).

| | Day followed the lives of individual women over fifteen years, and her book details their attempts to manage their lives, demonstrate autonomy and ability to make a living, look after family, etc. against a backdrop of social disapproval)

For discussions of cross-cultural psychology see e.g.: (Nisbett 2003) General on cross-cultural differences; and (Nisbett 1996) for discussion culture psychology and violence within the US South.

The notion of consumer culture, and cultural capital (Pierre Boudieu, *Distinction: A Social Critique of the Judgement of Taste,* 1979, Harvard University Press) is pertinent here. Notions of cultural values have been widely used (e.g. Daniel Miller, *The Comfort of Things*, 2008 Polity Press, explores how people use things to express themselves and make meaning in their lives, using things to build communities and social bonds; Lauren Berlant, *Cruel Optimism,* 2011 Duke University Press, looks at how people remain attached to the post-war promises of upward mobility, job security, political and social equality, and durable intimacy despite evidence to the contrary - laying themselves open to the influence of advertising campaigns that play back these culturally dominant assumptions); Beverly Skeggs, *Formations of Class and Gender: Becoming Respectable,* 1997 Sage, an empirical study of how poor women struggle with and against dominant (middle-class values) of respectability in the struggles and choices of their everyday lives). | *(b) Strategic culture*
Much work suggests the importance of strategic culture, even though how far it is measurable at the state level are debated (Booth, 1979; Katzenstein, 1996; Snyder, 1977; Sondhaus, 2006). |

EVIDENCE FOR CHAPTER 3 - MESSAGES

Concept	Communities and masses of individuals	State

(I) FASHIONING MESSAGES		
Simplicity [Para 3.3]	MODERATE Field studies in health: By analogy - (Jack et al. 2009) simple discharge plan RCT; (Gigerenzer 2008) heart simple decision tree; King et al., prescribing; (Gobet et al. 2001) chunking gives plausibility. Laboratory psychology experiments (Schwarz et al. 2007) and (Reber and Schwarz 1999) in (Cook and Lewandowsky, 2012). Further evidence in (Heath and Heath 2007).	N/A
Complete narrative (or, don't leave incomplete narratives) [Para 3.4]	MODERATE Compliance with asking favour of using photocopier more successful if give reason "because" (Langer et al., 1978). People like reasons (Bastardi and Shafir, 2000). Convergent evidence of causal models of the world (note models in World Bank 2015 world development report). Mainly laboratory psychology experiments and convergent psychological evidence, e.g. People prefer incorrect to incomplete explanations, reduced by adding plausible alternative (Ecker, Lewandowsky, and Tang 2010); in fictitious murder trials alternative suspect help (Tenney, Cleary, and Spellman 2009); preferred explanations are plausible and explain all (Seifert 2002); (Rapp and Kendeou 2007); (Cook and Lewandowsky, 2012).	N/A
Credible enough messages [Para 3.5] (Note that message credibility relates to messenger credibility, discussed under "Trust" in Ch 4)	STRONG Credibility in deterrence criminology. Deterrent messages: (Paternoster 2010) (Piquero et al. 2011) inter-individual differences. See also trust and credibility in Chapter 4 below.	STRONG Credibility widely seen as key to deterrence between states, e.g. (Freedman 2004; Morgan 2003). Credibility is also in the Chinese military textbook (Peng and Yao, 2005) Credibility is in the eye of the audience (Press 2004). Peng and Yao (2005) also discuss transmission. What increases credibility? Power and will. Reputation from past actions, and interests at stake in a given situation (problem of reassurance versus deterrence). Hence credibility of message and messenger is bound.

Language and symbols [Para 3.6]	STRONG Reviewed in (Gass and Seiter 2013) chapters 7 on linguistic and 8 on non-verbal communication. The audience must be able to sufficiently comprehend messages. Appropriate language and symbols also help other aspects of influence, e.g. establish similarity with an audience, authority (Cialdini 2008). Poorly constructed messages decrease credibility: (Sharp and McClung 1966; McCroskey and Mehrley 1969).	STRONG Help avoid: misinterpretation of signals from different operational codes or strategic cultures (Katzenstein 1996); and misinterpretation of signals between states, e.g. Chinese Leader Mao's 1960s/70s rapprochement with the US (Chen 2001).
Manage unexpectedness, creativity and novelty Para 3.7, 3.8]	STRONG Convergent evidence lab psych and neuroscience, e.g. (Wright 2015). (Bongar, Brown, and Beutler 2006) review volume on psychology and terrorism – gaining attention is key. Attention: (Cialdini 2008) p. 116 personalisation is important to gain attention, also shown more recently (Service et al 2014). Counterinsurgency, e.g. (Kilcullen 2013) theory of competitive control and expectation management.	STRONG Surprise and unexpectedness in diplomatic and military confrontations: (Handel 1980) (Handel 1981) (Betts 1982) (Betts and Mahnken 2004) (Mitchell 2000) (Vertzberger 1990) (Quester 1990) (Lambert 1995). Expectations in (Schelling 1966)
Oblique [Para 3.10]	MODERATE Mulgan (2009, p. 23) oblique and creative – examples of Australian little finger, car maintenance, truth campaign.	
(II) CONTENT OF MESSAGES		
Self-interest: see chapter 2		
Alternatives	STRONG Interviews with current and former Military Information Support Operations practitioners in the US. E.g. Need plausible alternatives for fear messaging, see references above.	STRONG E.g. Schelling (1966) Arms and Influence
Identity see chapter 2		
Fairness see chapter 2		
Norms [Para 3.21]	STRONG Cialdini (2008) describes multiple examples, e.g.: p. 99 "We view a behaviour as correct in a given situation to the degree that we see others performing it." Also Lun et al (2007, p. 101) Filmed examples powerful, even on kids. p. 113 Kitty Genovese incident and psychology studies based on concept. Social proof: (Muchink et al., 2007; Asch, 1951, 1955, 1956; Chudek & Henrich, 2011; Festinger, 1954; Fiedler & Juslin, 2006;	STRONG (Johnston 2007) Socialisation of China. (Katzenstein 1996) and key constructivists, e.g Alexander Wendt.

	Leary & Baumeister, 2000; Sherif & Sherif, 1956; Weiss, et al., 1964). Backfire: (Wakefield et al., 2010) show a recent U.S. antidrug campaign targeting youth may have unintentionally increased drug use by suggesting that it was commonplace. Teens took this message to mean that it was acceptable among their peers. The health information was ignored, but not the information about the social norm. See also familiarity backfire effect in Cook and Lewandowsky (2012)	
Reciprocity [Para 3.20]	STRONG Cialdini (2008) describes multiple examples, e.g.: p. 19 Kunz and Woolcott (1976) send out holiday greeting cards. p. 22 Regan (1971) gift of Coke and then more raffle tickets; p. 21 Netherlands help New Orleans; p. 34 Break reciprocity rule and one has distaste (Wedekind and Milikski, 2000), note also giving without opportunity to repay is also disliked in US, Jap and Sweden (Gergen et al 1975). Cross-cultural: Across 15, diverse small-scale cultures most people were conditional co-operators and reciprocated in economic games (Henrich et al. 2001). Also, in-depth interviews with highly experienced intelligence and investigative interviewers from the U.S. (Russano et al., 2014) and five Asian-Pacific jurisdictions (Goodman-Delahunty & Howes, in press) show that reciprocity is a common tactic, both to show respect and to determine the subject's needs, with the expectation that they would reciprocate with cooperation World Bank (2015) provides examples, e.g.: p. 10: Vasilaky et al. (2013); BenYishay and Mobarak. (2014).	STRONG E.g. (Haushofer et al., 2010) tit for tat in Israel-Palestine conflict.
Coherence of self [Para 3.23]	STRONG Reviewed by Cialdini (2008). Classic work on "cognitive dissonance."	N/A
Narratives / stories [Para 3.22]	STRONG (Braddock and Dillard 2016) Meta-analysis. Strategy in military, politics and business (Freedman 2013).	STRONG Macroeconomics: (Akerlof and Shiller 2009). Strategy in military, politics and business (Freedman 2013).

Scarcity [Para 3.24]	MODERATE (Cialdini 2008) but note reverse effects have been reported amongst East Asian participants in laboratory experiments (Nisbett 2003). If an individual believes that there is a limited opportunity to take an action, he is more likely to act (Cialdini & Sagarin, 2005; Mittone & Savadori, 2006). Scarcity increases the efficacy of social consensus: it implies social consensus that an item is desirable, and scarce because other people want it. Scarcity also burdens the decision-making process, resulting in reliance on heuristics (Knowledge & Linn, 2004). Scarcity has been used in time-limited offers of more favorable outcomes for subjects who admit or confess to a crime (Davis & O'Donohue, 2004; Davis, Leo, & Follette, 2010; Davis, Weaver, & Leo, 2007); although, when used in this manner, there is the risk of compliance rather than cooperation.	N/A
Choice of medium [Para 3.25]	MODERATE Interviews, e.g. marketing and media.	MODERATE Cross domain deterrence, e.g. (Schelling 1966). Use of back channels
(III) CONTEXT OF MESSAGES		
Contrast and sequences [Para 3.26]	STRONG Humans (and other organisms) are uniquely tuned to *contrast*; that is, to differences and changes of state. The impact of the contrast between a previous state and a current state operates at virtually every level of functioning, including sensory perceptions (e.g., Gibson, 1933), social perceptions (e.g., Holmes & Berkowitz, 1961), and motivations (e.g., Weinstein, 1972). This sensitivity likely has an evolutionary advantage, since it is a change in the environment that might mean threat or harm. *Contrast* can serve to enhance the efficacy of influence and counter-resistance strategies. Many influence tactics rely on some kind of contrast, and the contrast can be subtle: Burger (1986) showed that people were more likely to purchase a 75-cent cupcake with a free cookie than they were to purchase a cupcake and cookie in combination for 75 cents. Cialdini (2008) reviews a number of examples, e.g.: p. 39 Context – present zoo trip after more extreme request then 3 times as many	MODERATE Some classic work described contrast effects akin to prediction error, e.g. (Jervis, 1970; Schelling, 1966; Smoke, 1977).

	students volunteered (Cialdini et al 1975). Schwarzwald et al 1979 too extreme initial request is rejected. Thompson 1990 just exaggerated enough. P41 Liddy and Watergate. Contrast matters as contrast = expectation management and that matters because of violations of expectation i.e. PEs. P43 Rejection then retreat follow up, more showed up (85 v 50%) Miller et al 1976. P44-45 Benton et al 1972 negotiation led to more satisfaction and responsibility afterwards. Priming is another case. Priming is when exposure to one stimulus influences the response to another stimulus. For instance, to influence specific individuals, physical sensations can be used to unconsciously modify a target's cognition or emotion e.g.: Ijzerman & Semin (2009); Williams & Bargh (2008); Helzer & Pizarro (2011); Ackerman et al. (2010); Griffitt (1970); Hsiang et al., (2013); Dawson (in press). Other examples are reviewed by (World Bank 2015, p. 31), e.g.: Englich et al. (2006); Montier (2007); Schwarz et al. (1991).	
Timing [Para 3.27]	STRONG Cialdini (2008) reviews a number of examples, e.g.: p. 59 commitment, leanings initial can bias us towards consistent subsequent choices (Brownstein 2003, Brownstein et al 2004; Russo et al 2006). p. 61 Korean war POWs lenient policy, different to WW2. P63 Chinese used salami slice, "The US is not perfect". p. 63 momentum of compliance that induces later behaviours (Carducci et al 1989; Schwartz 1970). P64 small commitment and salami slice. p. 64 Freedman and Fraser 1966 Big front yard driver safety sign increase to 76% when two weeks before had agreed to small sign, and even occurred when had signed petition to "keep California beautiful". p. 66-7 Korea POWs Segal (1954). A review of deterrence in crime described no good evidence on the timeliness ("celerity") of punishment on deterrence (Paternoster 2010). Service et al. (2014) report. World Bank (2015) provide examples, e.g.: p. 13 Weekly text messages to remind patients to take their HIV drugs in Kenya,	MODERATE E.g. (Kriesberg and Thorson 1991)

	improved the rate of drug adherence to 53% from a baseline of 40%. p. 38: Shu and Gneezy (2010). p. 38: Barrera-Osorio, et al (2011).	
Rebound effects and overcoming them	MODERATE (a) When an audience is already sceptical, then presenting information can lead to 'rebound effects', where oppositional views become even more entrenched. E.g. Kahan. et al. (2012) on climate change; Macrae et al. (1993). MODERATE *(b) Overcome by increasing trust* See trust notes in Chapter 4. MODERATE *(c) Overcome by avoiding triggers* E.g. (Gass and Seiter, 2013) review includes avoiding triggering. MODERATE *(d) Overcome with self-affirmation* (Cohen and Sherman 2014) reviews evidence, including lab and field, from education, health and inter-group conflict resolution – main limitation a practical one on interventions typically have people write about core personal values.	N/A

EVIDENCE FOR CHAPTER 4 - MESSENGERS

Concept	Communities and masses of individuals	State
(I) CHARACTERISTICS OF MESSENGERS		
Trust and credibility [Para 4.3]	STRONG Importance of trust supported by numerous reviews and practitioner interviews. E.g. (Gass and Seiter 2013) review credibility in persuasion in chapter 4 and describe its core components of expertise, trustworthiness and goodwill. Those perceived as expert and/or trustworthy on a topic are more persuasive, particularly with subjects unable or unmotivated to process persuasive information (Hovland &	STRONG The concept of trust relates to reassurance, cooperation, predictability, confidence and credibility. There are also issues related to the levels of analysis (i.e. is it trust between leaders, bureaucracies or states?). International relations work on trust includes: (Kydd 2000) who examined trust, reassurance and cooperation in the ending of the Cold War; (Larson 2000) examined the Cold War; (Rathbun 2011) examines trust in the League of Nations, birth of the UN and NATO negotiation;

	Weiss, 1951; Wilson & Sherrell, 1993; Falomir-Pichastor et al., 2006).	(Booth and Wheeler 2007) discuss trust in the context of the security dilemma.
	Behavioural economics shows the importance of trust on behaviour in the lab, e.g. reviewed in (Camerer 2003). Related work in neuroscience and psychology describes putative neural bases and specific breakdowns in mental illness (Read Montague, Lohrenz, and Dayan 2015).	Macroeconomics:(Akerlof and Shiller 2009) pp. 11-13 discuss trust and confidence, and Chapter 1 concerns confidence and its multipliers.
	Counter credibility, e.g. attack others' credibility: Cook and Lewandowsky, 2012.	Credibility has been a key concern in thinking on deterrence throughout the Cold War and since. E.g. for a discussion of thinking over this period see (Freedman 2003).
	Advertising/marketing: E.g. (Pornpitakpan, 2004) reviews five decades of research on credibility on persuasion, which indicates the superiority of a high-credibility sources over a low-credibility source.	
	(Wilson and Sherrell 1993) conducted a meta-analysis of effect size of messenger characteristics (mostly lab studies with self-report measures rather than behaviour), showing the effect of trustworthiness (although expertise had an even larger effect).	
	Peace Research (key works include Deutsch, 1957; Mitchell, 2000).	
Authority and expertise [Para 4.4]	STRONG E.g. see reviews by (Cialdini 2008) or (Gass and Seiter, 2013). Cialdini (2008) provides examples, e.g.: P183 Coffee Sanka brand decaf; Robert Young played doctor on TV. Cialdini (2008) p. P184 also discusses Connotations of authority: (1) Titles, p185 Prof 2.5 inches taller (Wilson 1968), after election win become taller (Higham and Clement 1992). Tall men earn more and more likely to leadership (Chaiken 1986; Judge and Cabel 2004). Hofling et al 1966 study with nurses phoned up and they gave drug. Suit Lefkowitz, 1955 (2) Clothes P188 security guard	N/A

	Bickman 1974, Bushman, 1988. (3) Trappings Fancy car stop at green light Doob and Gross 1968.	
Liking and soft power (Para 4.5]	STRONG Reviewed by (Cialdini 2008). Establishing common ground is a means to both influence (Perloff, 2003) and relationship building (Collins & Miller, 1994); liking is increased by similarity and similarity increases liking (Byrne, 1971; Collisson & Howell, 2014; Sprecher, 2014). Even superficial or incidental similarities can have an impact, such as sharing a birthday (Miller, Downs, & Prentice, 1998), academic major (Platow, Mills, & Morrison, 2000), or university (Mackie et al., 1990). Liking is also influenced by attractiveness, flattery, cooperation, comparison with others, and behavioral mimicry (Cialdini, 2009). A caveat: although people tend to believe flattery and like those who provide it (Byrne, Rasche, & Kelley, 1974; Drachman, deCarufel, & Insko, 1978), ingratiation can backfire when it is clear that the flatter is a manipulation to achieve other goals (Jones & Wortman, 1973). Self-disclosure: Presentation of personal information to establish similarity and, independently, increase liking (Sprecher et al., 2013; Collins & Miller, 1994). Cross cultural work related for high-face concern (Zane, & Ku, 2014).] Incongruent self-disclosure (e.g. over disclosure that is atypical or awkward) can lead to a negative impression (Abell et al., 2006; Henretty & Levitt, 2010).	STRONG E.g. see original formulation and review of "soft power" (Nye, 2004).
Similarity [Para 4.6]	MODERATE Evidence from public health reviewed by Kreuter & McClure (2004) and other fields (e.g. Cialdini & Goldstein, 2004).	N/A
Manage messenger salience [Para 4.8]	MODERATE World Bank (2015) review a number of examples. Bombarded by information (Mulgan, 2009, p. 22).	MODERATE (Yarhi-Milo 2014) (Yarhi-Milo 2013) selective attention hypothesis, more vivid. Confirmation bias: (Jervis 1976) Chapter 4 cognitive consistency.
(II) CAPABILITIES OF MESSENGERS		
Media analysis [Para 4.9]	STRONG Evidence from interviews.	N/A

Language [Para 4.10]	STRONG Interviews. Language capability limitations hampering analysis and influence operations, e.g. Brooks (2015).	STRONG Evidence from interviews..
(III) NETWORKS		
Networks inside the audience [Para 4.12]	MODERATE Interview evidence.	MODERATE Interview evidence.
Networks - links outside the audience to be used as messengers {para 4.13]	STRONG Cialdini (2008) gives examples, e.g. p. 142 Tupperware party (Taylor, 1978); and strength of social bond twice as important as project (Frenzen and Davis, 1990). World Bank (2015) gives examples, e.g.: p. 45 (Baldassarri & Grossman, 2013).	MODERATE Interview evidence.
Opinion leaders [Para 4.14]	MODERATE Importance of opinion leaders, e.g. in Syrian foreign fighter networks Kings College London report (Carter, Maher, and Neumann 2014) or (Wood 2015). Opinion leaders: (Paluck and Shepherd 2012) Successfully reduce bullying in United States' school. Highly connected students and "highly salient" clique leaders participated in a program designed to broadcast students' experiences with and reactions to harassment and to facilitate public discussion on the issue. The "social referents" wrote and read aloud essays about harassment, performed skits demonstrating the emotional effects of bullying, and sold wristbands signaling the wearers' commitment to reducing harassment. Changing the behavior of social referents changed peers' perceptions of schools' collective norms as well as actual harassment behavior through the mechanism of "everyday interaction". "Norm entrepreneurs" can alert people to the existence of a shared complaint and suggest collective solutions (Sunstein 1996; see also chapter 8 for an example involving quitting smoking).	N/A

	In health, various reviews support use of opinion leaders, although there is debate (https://www.nice.org.uk/Media/Default/About/what-we-do/Into-practice/Support-for-service-improvement-and-audit/Kings-Fund-literature-review.pdf). Methods to identify opinion leaders in health are reviewed by (Valente and Pumpuang, 2007).	
(IV) FINDING AND DEVELOPING TRUSTED MESSENGERS		
Finding trusted messengers [Para 4.15, 4.16, 4.17]	STRONG Online e.g. (Singer & Brooking, 2018; Singer & Friedman, 2014). CIA Italian-American operation cited in main text.	STRONG E.g. pre-WWI European Royal Families, other dynasties in the contemporary world (e.g. Kim family in the DPRK, leading Chinese or US families).
Develop trusted messengers [Para 4.18. 4.19, 4.20, 4.21]	STRONG *(a) Mass communication to populations* E.g. Trust surveys of BBC etc. cited in text. LOW *(b) Within local communities enhance status of specific individuals* Limited evidence, e.g. cited in text.	N/A
(V) COMPETING WITH OTHERS		
Resources matter – heavy investments, cheap asymmetric strategies and high-level policy support [Para 4.26, 4.27, 4.28]	STRONG Tailored Online Interventions: The Islamic State's Recruitment Strategy, JM Berger https://www.ctc.usma.edu/posts/tailored-online-interventions-the-islamic-states-recruitment-strategy ISIS Social Media Strategy http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/ Foreign Jihadists in Syria: Tracking Recruitment Networks https://www.washingtoninstitute.org/policy-analysis/view/foreign-jihadists-in-syria-tracking-recruitment-networks. Measuring influence, evaluating content and countering violent extremism in online social networks, ICSR	STRONG See Chapter 4 and Part III of this report for discussion of Chinese and Russian approaches.

	http://icsr.info/wp-content/uploads/2013/03/ICSR_Berger-and-Strathearn.pdf	
Other countries' understanding of influence Para 4.30, 4.31]	STRONG Giles and Hagestad (2013) compare Chinese, Russian and Euratlantic approaches. See Chapter 4 and Part III of this report for discussion of Chinese and Russian approaches.	STRONG Giles and Hagestad (2013) compare Chinese, Russian and Euratlantic approaches. See Chapter 4 and Part III of this report for discussion of Chinese and Russian approaches.
Agility [Para 4.32, 4.33]	STRONG Management literature and interviews. See e.g. references in text and for "outside-in."	STRONG Management literature and interviews. See e.g. references in text and for "outside-in."

REFERENCES FOR EVIDENCE TABLES

Abell, J., Locke, A., Condor, S., Gibson, S., & Stevenson, C. 2006. Trying similarity, doing difference: the role of interviewer self-disclosure in interview talk with young people. *Qualitative Research*. 6 (2): 221–244. http://doi.org/10.1177/1468794106062711

Ackerman, J. M., Nocera, C. C., & Bargh, J. A. 2010. Incidental haptic sensations influence social judgments and decisions. *Science*. 328: 1712–1715.

Akerlof, G. A, and R. J Shiller. 2009. *Animal Spirits*. Princeton, NJ: Princeton University Press.

Albin, Cecilia. 2001. *Justice and Fairness in International Negotiation*. Cambridge University Press.

Alkis, N, Taskaya Temizel, T. 2015. "The impact of individual differences on influence strategies". Personality and Individual Differences. 87: 147-152.

Anthes, Emily. 2015. "Hospital Checklists Are Meant to Save Lives — so Why Do They Often Fail?" *Nature News* 523 (7562): 516. doi:10.1038/523516a.

Ashraf, Nava, Oriana Bandiera, and B. Kelsey Jack. 2014. "No Margin, No Mission? A Field Experiment on Incentives for Public Service Delivery." *Journal of Public Economics* 120: 1–17.

Barrera-Osorio, Felipe, Marianne Bertrand, Leigh L. Linden, and Francisco Perez-Calle. 2011. "Improving the Design of Conditional Transfer Programs: Evidence from a Randomized Education Experiment in Colombia." *American Economic Journal: Applied Economics*. 3 (2): 167–95.

Bastardi, A., & Shafir, E. 2000. Nonconsequential reasoning and its consequences. Current Directions in Psychological Science, 9(6), 216-219.

Bauman, Gerd. 1996. *Contesting Culture*. Cambridge University Press

Bazerman, Max H., Jared R. Curhan, Don A. Moore, and Kathleen L. Valley. 2000. "Negotiation." *Annual Review of Psychology* 51 (1): 279–314. doi:10.1146/annurev.psych.51.1.279.

BenYishay, Ariel, and A. Mushfiq Mobarak. 2014. "Social Learning and Communication." Working Paper 20139, National Bureau of Economic Research, Cambridge, MA.

Berlant, Lauren. 2011. *Cruel Optimism.* Duke University Press

Berns, Gregory S., Emily Bell, C. Monica Capra, Michael J. Prietula, Sara Moore, Brittany Anderson, Jeremy Ginges, and Scott Atran. 2012. "The Price of Your Soul: Neural Evidence for the Non-Utilitarian Representation of Sacred Values." *Philosophical Transactions of the Royal Society B: Biological Sciences* 367 (1589): 754–762.

Besley, Timothy, and Maitreesh Ghatak. 2008. "Status Incentives." *The American Economic Review* 98 (2): 206–211.

Betts, Richard K. 1982. *Surprise Attack: Lessons for Defense Planning*. Brookings Institution Press.

Betts, Richard K., and Thomas Mahnken. 2004. *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*. Routledge.

Blatt, Benjamin, Susan F. LeLacheur, Adam D. Galinsky, Samuel J. Simmens, and Larrie Greenberg. 2010. "Does Perspective-Taking Increase Patient Satisfaction in Medical Encounters?:" *Academic Medicine* 85 (9): 1445–52. doi:10.1097/ACM.0b013e3181eae5ec.

Bongar, Bruce, Lisa M. Brown, and Larry E. Beutler, eds. 2006. *Psychology of Terrorism*. 1 edition. Oxford ; New York: Oxford University Press.

Booth, K. 1979. *Strategy and Ethnocentrism*. NY: Holmes & Meier.

Booth, Ken, and Nicholas Wheeler. 2007. *Security Dilemma: Fear, Cooperation, and Trust in World Politics*. First Edition edition. Basingstoke England ; New York, N.Y: Palgrave Macmillan.

Boudieu, Pierre. 1979. *Distinction: A Social Critique of the Judgement of Taste.* Harvard University Press.

Bourdieu, Pierre. 1977. *Outline of a Theory of Practice*. Cambridge, U.K.: Cambridge University Press.

Bowen, John R. 2008. *Why the French Don't Like Headscarves: Islam, the State, and Public Space*. Princeton University Press.

Braddock, Kurt, and James Price Dillard. 2016. "Meta-Analytic Evidence for the Persuasive Effect of Narratives on Beliefs, Attitudes, Intentions, and Behaviors." *Communication Monographs* 0 (0): 1–24. doi:10.1080/03637751.2015.1128555.

Brooks, R. 2015. Obama: The last year and the Legacy, *Foreign Policy*, Feb 25th

Camerer, C. F. 2003. "Strategizing in the Brain." *Science* 300 (5626): 1673.

Camerer, Colin F. 2003. *Behavioral Game Theory: Experiments in Strategic Interaction*. Vol. 9. Princeton University Press Princeton, NJ.

Cameron, Kenzie A. 2009. "A Practitioner's Guide to Persuasion: An Overview of 15 Selected Persuasion Theories, Models and Frameworks." *Patient Education and Counseling* 74 (3): 309–17. doi:10.1016/j.pec.2008.12.003.

Carter, Joseph A., Shiraz Maher, and Peter R. Neumann. 2014. "# Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks." http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.662.1555.

Chen, Jian. 2001. *Mao's China and the Cold War*. 1 edition. Chapel Hill: The University of North Carolina Press.

Christensen, Thomas J. 1999. "China, the U.S.-Japan Alliance, and the Security Dilemma in East Asia." *International Security* 23 (4): 49–80.

———. 2015. *The China Challenge: Shaping the Choices of a Rising Power*. W. W. Norton & Company.

Cialdini, Robert B. 2008a. *Influence: Science and Practice*. 5th ed. Boston: Pearson.

Cialdini, Robert B., & Goldstein, N. J. 2004. Social influence: compliance and conformity. *Annual Review of Psychology*, *55*: 591–621. https://doi.org/10.1146/annurev.psych.55.090902.142015

Cohen, Geoffrey L., and David K. Sherman. 2014. "The Psychology of Change: Self-Affirmation and Social Psychological Intervention." *Annual Review of Psychology* 65: 333–371.

Cohn, Alain, Michel André Maréchal, and Thomas Noll. 2013. "Bad Boys: The Effect of Criminal Identity on Dishonesty." Working Paper 132, University of Zurich, Zurich.

Collins, N. L., & Miller, L. C. 1994. Self-disclosure and liking: a meta-analytic review. *Psychological Bulletin*, *116* (3): 457–475.

Darnton, A. 2008. "GSR Behaviour Change Knowledge Review: Overview of Behaviour Change Models and Their Uses-Briefing Note for Policy Makers." Government Social Research Unit.

Day, Sophie. 2007. *On the Game: Women and Sex Work*. Pluto Press.

Day, and Moorman. 2010. *Strategy from the Outside In: Profiting from Customer Value*. New York: McGraw-Hill Professional.

Dawson, E., Hartwig, M., & Brimbal, L. (in press). Interviewing to Elicit Information: Using Priming to Promote Disclosure. *Law and Human Behavior*.

Denrell, J., & Le Mens, G. 2007. Interdependent sampling and social influence. Psychological Review. 114: 398–422.

DiMaggio, Paul. 1997. "Culture and Cognition." *Annual Review of Sociology* 23 (1): 263–87.

Dolan, Paul, Michael Hallsworth, David Halpern, Dominic King, and Ivo Vlaev. 2010. "MINDSPACE: Influencing Behaviour Through Public Policy." Institute for Government.

Douglas, Mary. 1970, *Natural symbols, explorations in cosmology*. Penguin.

Ecker, Ullrich K. H., Stephan Lewandowsky, and David T. W. Tang. 2010. "Explicit Warnings Reduce but Do Not Eliminate the Continued Influence of Misinformation." *Memory & Cognition* 38 (8): 1087–1100. doi:10.3758/MC.38.8.1087.

Ellsworth, Richard R. 2002. *Leading with Purpose: The New Corporate Realities*. Stanford University Press.

Englich, Birte, Thomas Mussweiler, and Fritz Strack. 2006. "Playing Dice with Criminal Sentences: The Influence of Irrelevant Anchors on Experts' Judicial Decision Making." *Personality and Social Psychology Bulletin* 32 (2): 188–200.

Frank, Robert H. 1985. *Choosing the Right Pond: Human Behaviour and the Quest for Status* (New York: Oxford University Press)

Frank, Robert H. 1999. *Luxury Fever: Why Money Fails to Satisfy in an Era of Excess* (New York: Free Press)

Frank, Robert H. 2005. "Positional Externalities Cause Large and Preventable Welfare Losses," *American Economic Review* 95

Freedman, J. L. (1965). Long-term behavioral effects of cognitive dissonance. *Journal of Experimental Social Psychology*, 1(2), 145-155.

Freedman, Lawrence. 2003. *The Evolution of Nuclear Strategy*. 3rd edition. Palgrave Macmillan.

———. 2004. *Deterrence*. 1 edition. Cambridge, UK ; Malden, MA: Polity.

Freedman, Sir Lawrence. 2013. *Strategy: A History*. Oxford ; New York: OUP USA.

Fukuyama, Francis. 2014. *Political Order and Political Decay: From the Industrial Revolution to the Globalisation of Democracy*. Profile Books.

Galinsky, Adam D., William W. Maddux, Debra Gilin, and Judith B. White. 2008. "Why It Pays to Get inside the Head of Your Opponent the Differential Effects of Perspective Taking and Empathy in Negotiations." *Psychological Science* 19 (4): 378–384.

Gambetta, D. & Hertog, S. 2016. Engineers of Jihad: The Curious Connection between Violent Extremism and Education. Princeton University Press.

Gass, Robert H., and John S. Seiter. 2013. *Persuasion: Social Influence and Compliance Gaining*. 5 edition. Boston: Routledge.

Gawande, Atul. 2009. *The Checklist Manifesto: How to Get Things Right*. First Edition edition. New York: Metropolitan Books.

Gigerenzer, Gerd. 2008. *Gut Feelings: Short Cuts to Better Decision Making*. Penguin.

Gobet, Fernand, Peter CR Lane, Steve Croker, Peter CH Cheng, Gary Jones, Iain Oliver, and Julian M. Pine. 2001. "Chunking Mechanisms in Human Learning." *Trends in Cognitive Sciences* 5 (6): 236–243.

Gray, Colin S. 2003. "Maintaining Effective Deterrence." DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA417180.

Gries, Peter Hays. 2004a. *China's New Nationalism: Pride, Politics, and Diplomacy*. Berkeley, Calif.: Univ. of California Press.

Griffitt, W. 1970. Environmental effects on interpersonal affective behaviour: Ambient effective temperature and attraction. *Journal of Personality and Social Psychology*, 15: 240-244.

Gulati, Ranjay. 2010. *Reorganize for Resilience: Putting Customers at the Center of Your Business*. Boston, Mass: Harvard Business School Press.

Haas, Mark L. 2001a. "Prospect Theory and the Cuban Missile Crisis." *International Studies Quarterly* 45 (2): 241–70.

Handel, Michael I. 1980. "Surprise and Change in International Politics." *International Security* 4 (4): 57–85. doi:10.2307/2626668.

———. 1981. *The Diplomacy of Surprise, Hitler, Nixon, Sadat*. Center for International Affairs, Harvard University.

Haushofer, Johannes, Anat Biletzki, and Nancy Kanwisher. 2010. "Both Sides Retaliate in the Israeli–Palestinian Conflict." *Proceedings of the National Academy of Sciences*, October. doi:10.1073/pnas.1012115107.

Heath, Chip, and Dan Heath. 2007. *Made to Stick: Why Some Ideas Survive and Others Die*. 1st edition. New York: Random House.

Helzer, E. G., & Pizarro, D. A. 2011. Dirty Liberals! Reminders of Physical Cleanliness Influence Moral and Political Attitudes. *Psychological Science*, 22: 517–522.

Henretty, J. R., & Levitt, H. M. 2010. The role of therapist self-disclosure in psychotherapy: A qualitative review. Clinical Psychology Review. 30 (1): 63–77. http://doi.org/10.1016/j.cpr.2009.09.004

Henrich, Joseph, Robert Boyd, Samuel Bowles, Colin Camerer, Ernst Fehr, Herbert Gintis, and Richard McElreath. 2001a. "In Search of Homo Economicus: Behavioral Experiments in 15 Small-Scale Societies." *The American Economic Review* 91 (2): 73–78.

Herzfeld, Michael. 2005. *Cultural intimacy: Social poetics in the nation-state*.

Hirsh, J. B., Kang, S. K., & Bodenhausen, G. V. 2012. Personalized persuasion tailoring persuasive appeals to recipients' personality traits. *Psychological science*, *23* (6): 578-581.

Hoff, Karla, and Priyanka Pandey. 2006. "Discrimination, Social Identity, and Durable Inequalities." *The American Economic Review* 96 (2): 206–211.

———. 2014. "Making up People—the Effect of Identity on Performance in a Modernizing Society." *Journal of Development Economics* 106: 118–131.

Hopf, Ted. 2002. *Social Construction of Foreign Policy: Identities and Foreign Policies, Moscow, 1955 and 1999*. Ithaca: Cornell University Press.

Huntington, Samuel P. 2002. *The Clash Of Civilizations: And The Remaking Of World Order*. Reissue edition. Simon & Schuster UK.

Horowitz, M., McDermott, R., & Stam, A. C. (2005). *Leader Age, Regime Type, and Violent International Relations*. The Journal of Conflict Resolution, 49(5), 661–685.

Hsiang, S. M., Burke, M., & Miguel, E. 2013. Quantifying the influence of climate on human conflict. *Science*. 341: 1212.

Ijzerman, H., & Semin, G. R. 2009. The Thermometer of Social Relations Mapping Social Proximity on Temperature. *Psychological Science*, 20: 1214–1220.

Jack, Brian W., Veerappa K. Chetty, David Anthony, Jeffrey L. Greenwald, Gail M. Sanchez, Anna E. Johnson, Shaula R. Forsythe, et al. 2009. "A Reengineered Hospital Discharge Program to Decrease Rehospitalization: A Randomized Trial." *Annals of Internal Medicine* 150 (3): 178–187.

Jervis, Robert. 1970. *The Logic of Images in International Relations*. Princeton University Press.

———. 1976. *Perception and Misperception in International Politics*. Vol. 49. Princeton University Press. http://books.google.co.uk/books?hl=en&lr=&id=qqAIuHgi2hoC&oi=fnd&pg=PA3&dq=jervis+perception+and+misperception&ots=7TziEjMmZh&sig=ve0myfEnm8RD41rNelJ-LbwYsAc.

———. 1992a. "Political Implications of Loss Aversion." *Political Psychology* 13 (2): 187–204.

———. 2001. "Was the Cold War a Security Dilemma?" *Journal of Cold War Studies* 3 (1): 36–60. doi:10.1162/15203970151032146.

Johnston, Alastair Iain. 2007. *Social States: China in International Institutions, 1980-2000*. Princeton University Press.

Kagel, J.H., and A.E. Roth. 1995. "The Handbook of Experimental Economics." *Princeton, NJ*.

Kahneman, D., and A. Tversky. 1979. "Prospect Theory: An Analysis of Decision under Risk." *Econometrica: Journal of the Econometric Society*, 263–291.

Kapferer, Bruce. 1988. *Legends of People, Myths of State*. Smithsonian Institution Press.

Katzenstein, Peter J. 1996. *The Culture of National Security: Norms and Identity in World Politics*. Columbia University Press.

Kilcullen, David. 2013. *Out of the Mountains: The Coming Age of the Urban Guerrilla*. Oxford ; New York, NY: Oxford University Press.

Kirca, Ahmet H., Satish Jayachandran, and William O. Bearden. 2005. "Market Orientation: A Meta-Analytic Review and Assessment of Its Antecedents and Impact on Performance." *Journal of Marketing* 69 (2): 24–41.

Kleinman, Arthur. 2006. *What Really Matters: Living a Moral Life amidst Uncertainty and Danger.* Oxford, U.K.: Oxford University Press.

Knopf, Jeffrey W. 2010a. "The Fourth Wave in Deterrence Research." *Contemporary Security Policy* 31 (1): 1–33.

———. 2012. "Nuclear Disarmament and Nonproliferation: Examining the Linkage Argument."
http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00109.

Kohn, Alfie. 2000. *Punished by Rewards: The Trouble with Gold Stars, Incentive Plans, A's, Praise and Other Bribes*. Boston: Houghton Mifflin.

Kosfeld, Michael, and Susanne Neckermann. 2011. "Getting More Work for Nothing? Symbolic Awards and Worker Performance." *American Economic Journal: Microeconomics*, 86–99.

Kreuter, Matthew W., and Stephanie M. McClure. 2004. "The Role of Culture in Health Communication." *Annual Review of Public Health* 25 (1): 439–55. doi:10.1146/annurev.publhealth.25.101802.123000.

Kriesberg, Louis, and Stuart J. Thorson. 1991. *Timing and the De-Escalation of International Conflicts*. Syracuse University Press.

Kydd, Andrew. 2000. "Trust, Reassurance, and Cooperation." *International Organization* 54 (2): 325–357. doi:10.1162/002081800551190.

Kydd, Andrew H. 2005. *Trust And Mistrust In International Relations*. Princeton University Press.

Lambert, A. P. N. 1995. *The Psychology of Air Power*. London: Royal United Services Institute for Defence Studies.

Langer, E. J., Blank, A., & Chanowitz, B. (1978). The mindlessness of ostensibly thoughtful action: The role of" placebic" information in interpersonal interaction. Journal of personality and social psychology, 36(6), 635.

Larkin, Ian. 2011. "Paying $30,000 for a Gold Star: An Empirical Investigation into the Value of Peer Recognition to Software Salespeople." *Mimeo*.

Larson, Deborah Welch. 2000. *Anatomy of Mistrust: U.S.-Soviet Relations During the Cold War*. Ithaca, NY: Cornell University Press.

Larson, Deborah Welch, and Alexei Shevchenko. 2010a. "Status Seekers: Chinese and Russian Responses to US Primacy." *International Security* 34 (4): 63–95.

Levine, M., Prosser, A., Evans, D.& Reicher, S. 2005. Identity and Emergency Intervention: How Social Group Membership and Inclusiveness of Group Boundaries Shapes Helping Behavior. *Personality and Social Psychology Bulletin*, 31 (4): 443-453.

Loch, C., Yaziji, M. and Langen, C. 2001. "The Fight for the Alpha Position: Channeling Status Competition in Organizations," *European Management Journal.* 19

Macrae, C. N. et al. 1993. "Out of mind but back in sight: stereotypes on the rebound". *Journal of Personality and Social Psychology*. 67: 808-917.

Maio, Gregory R., and Geoff Haddock. 2009. *The Psychology of Attitudes and Attitude Change*. Los Angeles ; London: Sage Publications Ltd.

Malhotra, Deepak, and Max Bazerman. 2012. *Negotiation Genius: How to Overcome Obstacles and Achieve Brilliant Results at the Bargaining Table and Beyond*. Reprint edition. Bantam Books Inc.

Maloney, Erin K., Maria K. Lapinski, and Kim Witte. 2011. "Fear Appeals and Persuasion: A Review and Update of the Extended Parallel Process Model." *Social and Personality Psychology Compass* 5 (4): 206–19. doi:10.1111/j.1751-9004.2011.00341.x.

McCroskey, James C., and R. Samuel Mehrley. 1969. "The Effects of Disorganization and Nonfluency on Attitude Change and Source Credibility." *Communications Monographs* 36 (1): 13–21.

McDermott, Rose. 2001a. *Risk-Taking in International Politics: Prospect Theory in American Foreign Policy*. University of Michigan Press.

Mercer, J. 2005a. "Prospect Theory and Political Science." *Annual Review of Political Science* 8: 1–21.

Michie, Susan, Maartje M. van Stralen, and Robert West. 2011. "The Behaviour Change Wheel: A New Method for Characterising and Designing Behaviour Change Interventions." *Implementation Science* 6 (1): 42.

Miguéis, Vera L., Ana S. Camanho, and João Falcão e Cunha. 2012. "Customer Data Mining for Lifestyle Segmentation." *Expert Systems with Applications* 39 (10): 9359–9366.

Miller, Daniel. 2008. *The Comfort of Things*. Polity Press

Mitchell, Christopher Roger. 2000. *Gestures of Conciliation: Factors Contributing to Successful Olive Branches*. St. Martin's Press.

Montier, James. 2007. *Applied Behavioural Finance.* Chichester, England: Wiley.

Morgan, Neil A., Douglas W. Vorhies, and Charlotte H. Mason. 2009. "Market Orientation, Marketing Capabilities, and Firm Performance." *Strategic Management Journal* 30 (8): 909–920.

Morgan, Patrick M. 2003. *Deterrence Now*. Cambridge University Press.

Muchink, L., Aral, S., & Taylor, S. J. 2013. Social influence bias: A randomized experiment. *Science*, 341: 647–651.

Munoz, Arturo. 2012. *U.S. Military Information Operations in Afghanistan*. Rand Corp.

Nincic, Miroslav. 2010a. "Getting What You Want: Positive Inducements in International Relations." *International Security* 35 (1): 138–83. doi:10.1162/ISEC_a_00006.

Nisbett, Richard. 2003. *The Geography of Thought: How Asians and Westerners Think Differently...and Why*. 1St Edition edition. New York: Free Press.

Nisbett, Richard E. 1996. *Culture Of Honor: The Psychology Of Violence In The South*. Boulder, Colo: Westview Press.

———. 2003. *The Geography of Thought: How Asians and Westerners Think Differently - And Why*. New Edition edition. Nicholas Brealey Publishing.

Nye, Joseph S. 2004a. *Soft Power: The Means to Success in World Politics*. 1st ed. New York: Public Affairs.

Paluck, Elizabeth Levy, and Hana Shepherd. 2012. "The Salience of Social Referents: A Field Experiment on Collective Norms and Harassment Behavior in a School Social Network." *Journal of Personality and Social Psychology* 103 (6): 899.

Paternoster, Raymond. 2010. "How Much Do We Really Know about Criminal Deterrence?" *The Journal of Criminal Law and Criminology*, 765–824.

Payne, Keith B. 2001. *The Fallacies of Cold War Deterrence and a New Direction*. Lexington: University Press of Kentucky.

Peng, Guangqian, and Youzhi Yao. 2005. *The Science of Military Strategy*. Beijing: Military Science Publishing House.

Piquero, Alex R., Raymond Paternoster, Greg Pogarsky, and Thomas Loughran. 2011. "Elaborating the Individual Difference Component in Deterrence Theory." *Annual Review of Law and Social Science* 7 (1): 335–60. doi:10.1146/annurev-lawsocsci-102510-105404.

Pornpitakpan, Chanthika. 2004. "The Persuasiveness of Source Credibility: A Critical Review of Five Decades' Evidence." *Journal of Applied Social Psychology* 34 (2): 243–81. doi:10.1111/j.1559-1816.2004.tb02547.x.

Posen, Barry R. 1993. "The Security Dilemma and Ethnic Conflict." *Survival* 35 (1): 27–47. doi:10.1080/00396339308442672.

Press, Daryl G. 2004. "The Credibility of Power: Assessing Threats during the 'Appeasement' Crises of the 1930s." *International Security* 29 (3): 136–69.

Promberger, Marianne, and Theresa M. Marteau. 2013. "When Do Financial Incentives Reduce Intrinsic Motivation? Comparing Behaviors Studied in Psychological and Economic Literatures." *Health Psychology* 32 (9): 950.

Quester, George H. 1990. "The Psychological Effects of Bombing on Civilian Populations : Wars of the Past." In *Psychological Dimensions of War*, edited by Betty Glad. SAGE Publications, Inc.

Quinlan, M. 2004. "Deterrence and Deterrability." *Contemporary Security Policy* 25: 11–17.

Rapp, David N., and Panayiota Kendeou. 2007. "Revising What Readers Know: Updating Text Representations during Narrative Comprehension." *Memory & Cognition* 35 (8): 2019–2032.

Rathbun, Brian C. 2011. *Trust in International Cooperation: International Security Institutions, Domestic Politics and American Multilateralism*. London: Cambridge University Press.

Read Montague, P, Terry Lohrenz, and Peter Dayan. 2015. "The Three R's of Trust." *Current Opinion in Behavioral Sciences*, Social behavior, 3 (June): 102–6. doi:10.1016/j.cobeha.2015.02.009.

Reber, Rolf, and Norbert Schwarz. 1999. "Effects of Perceptual Fluency on Judgments of Truth." *Consciousness and Cognition* 8 (3): 338–342.

Reicher, S., Cassidy, C., Hopkins, N. & Levine, M. 2006. Saving Bulgaria's Jews: An analysis of social identity and the mobilisation of social solidarity *European Journal of Social Psychology*, 36 (1): 49-72.

Rosen, Stephen Peter. 2005. *War and Human Nature* (Princeton: Princeton University Press)

Ruiter, Robert AC, Charles Abraham, and Gerjo Kok. 2001. "Scary Warnings and Rational Precautions: A Review of the Psychology of Fear Appeals." *Psychology and Health* 16 (6): 613–630.

Schaub, Gary. 2004a. "Deterrence, Compellence, and Prospect Theory." *Political Psychology* 25 (3): 389–411.

Schelling, Thomas Crombie. 1966. *Arms and Influence*. Yale University Press.

Schwarz, Norbert, Fritz Strack, and Hans-Peter Mai. 1991. "Assimilation and Contrast Effects in Part-Whole Question Sequences: A Conversational Logic Analysis." *Public Opinion Quarterly* 55 (1): 3–23.

Schwarz, Norbert, Lawrence J. Sanna, Ian Skurnik, and Carolyn Yoon. 2007. "Metacognitive Experiences and the Intricacies of Setting People Straight: Implications for Debiasing and Public Information Campaigns." *Advances in Experimental Social Psychology* 39: 127.

Seifert, Colleen M. 2002. "The Continued Influence of Misinformation in Memory: What Makes a Correction Effective?" *Psychology of Learning and Motivation* 41: 265–294.

Service, Owain, Michael Hallsworth, David Halpern, Felicity Algate, Rory Gallagher, Sam Nguyen, Simon Ruda, et al. 2014. "EAST: Four Simple Ways to Apply Behavioural Insights." The Behavioural Insights Team.

Shambaugh, David. 2013a. *China Goes Global: The Partial Power*. New York: Oxford University Press.

Sharp Jr, Harry, and Thomas McClung. 1966. "Effects of Organization on the Speaker's Ethos." http://www.tandfonline.com/doi/pdf/10.1080/03637756609375495.

Sherif, Muzafer, Oliver J. Harvey, B. Jack White, William R. Hood, Carolyn W. Sherif, and others. 1961. *Intergroup Conflict and Cooperation: The Robbers Cave Experiment*. Vol. 10. University Book Exchange Norman, OK.

Shu, Suzanne B., and Ayelet Gneezy. 2010. "Procrastination of Enjoyable Experiences." *Journal of Marketing Research* 47 (5): 933–44.

Singer, P. W., & Brooking, E. T. 2018. *LikeWar: The Weaponization of Social Media*. Houghton Mifflin Harcourt.

Singer, P. W., & Friedman, A. 2014. *Cybersecurity and Cyberwar What Everyone Needs to Know*. Oxford ; New York: Oxford University Press, USA.

Skeggs, Beverly. 1997. *Formations of Class and Gender: Becoming Respectable.* Sage

Smoke, Richard. 1977. *War: Controlling Escalation*. Harvard University Press.

Sniehotta, Falko F., Justin Presseau, and Vera Araújo-Soares. 2014. "Time to Retire the Theory of Planned Behaviour." *Health Psychology Review* 8 (1): 1–7. doi:10.1080/17437199.2013.869710.

Snyder, J. L. 1977. *The Soviet Strategic Culture : Implications for Limited Nuclear Operations.* Santa Monica, Calif.: Rand Corporation. Retrieved from http://www.rand.org/pubs/reports/R2154.html

Soames Job, R. F. 1988. "Effective and Ineffective Use of Fear in Health Promotion Campaigns." *American Journal of Public Health* 78 (2): 163–167.

Solomon, R. H. 1995. Chinese Political Negotiating Behavior, 1967-1984. Retrieved January 18, 2013, from http://www.rand.org/pubs/monograph_reports/MR663.html

Sondhaus, L. 2006. *Strategic Culture and Ways of War*. Taylor & Francis.

Spangler, Stanley E. 1991a. *Force and Accommodation in World Politics*. DIANE Publishing.

Sprecher, S., Treger, S., Wondra, J. D., Hilaire, N., & Wallpe, K. 2013. Taking turns: Reciprocal self-disclosure promotes liking in initial interactions. *Journal of Experimental Social Psychology. 49* (5): 860–866.

Stein, Janice Gross, and Louis W. Pauly. 1992a. "Choosing to Co-Operate: How States Avoid Loss." *International Journal* 47 (2): 199. doi:10.2307/40202758.

Steinberg, James, and Michael E. O`Hanlon. 2014. *Strategic Reassurance and Resolve: U.S.-China Relations in the Twenty-First Century*. Princeton, New Jersey: Princeton University Press.

Steinberg, Laurence. 2004. "Risk Taking in Adolescence: What Changes, and Why?" *Annals of the New York Academy of Sciences* 1021 (1): 51–58. doi:10.1196/annals.1308.005.

Tannenbaum, Melanie B., Justin Hepler, Rick S. Zimmerman, Lindsey Saul, Samantha Jacobs, Kristina Wilson, and Dolores Albarracín. 2015. "Appealing to Fear: A Meta-Analysis of Fear Appeal Effectiveness and Theories." *Psychological Bulletin* 141 (6): 1178.

Taylor, John, Professor Adrian Furnham, and Janet Breeze. 2014. *Revealed: Using Remote Personality Profiling to Influence, Negotiate and Motivate*. New York: Palgrave Macmillan.

Tenney, Elizabeth R., Hayley MD Cleary, and Barbara A. Spellman. 2009. "Unpacking the Doubt in 'Beyond a Reasonable Doubt': Plausible Alternative Stories Increase Not Guilty Verdicts." *Basic and Applied Social Psychology* 31 (1): 1–8.

Turner, John C. 1985. "Social Categorization and the Self-Concept: A Social Cognitive Theory of Group Behavior". *Advances in Group Process: Theory and Research.* 2: 77–122. Greenwich, CT: JAI Press.

Tversky, A., and D. Kahneman. 1992. "Advances in Prospect Theory: Cumulative Representation of Uncertainty." *Journal of Risk and Uncertainty* 5 (4): 297–323.

Valente, Thomas W., and Patchareeya Pumpuang. 2007. "Identifying Opinion Leaders to Promote Behavior Change." *Health Education & Behavior*. http://heb.sagepub.com/content/early/2007/06/29/1090198106297855.short.

Vasilaky, Kathryn, and Kenneth L. Leonard. 2013. "As Good as the Networks They Keep? Improving Farmers' Social Networks via Randomized Information Exchange in Rural Uganda." Working Paper, University of Maryland, College Park.

Verdery. 1999. *The Political Lives of Dead Bodies: Reburial and Postsocialist Change*. Columbia University Press

Vertzberger, Yaacov. 1990. *The World in Their Minds: Information Processing, Cognition, Perception in Foreign Policy Decisionmaking*. Stanford University Press.

Wakefield, Melanie A., Barbara Loken, and Robert C. Hornik. 2010. "Use of Mass Media Campaigns to Change Health Behaviour." *The Lancet* 376 (9748): 1261–1271.

Waldron, Vincent R., and James L. Applegate. 1998. "Person-Centered Tactics during Verbal Disagreements: Effects on Student Perceptions of Persuasiveness and Social Attraction." *Communication Education* 47 (1): 53–66.

Wang, Zheng. 2012. *Never Forget National Humiliation: Historical Memory in Chinese Politics and Foreign Relations*. New York: Columbia University Press.

Wheeler, Michael O. 2003. "Nuclear Deterrence Issues in the Post-September 11 World: An American Perspective." *Nuclear Issues in the Post-September 11 Era, Recherches & Documents* 30 (Fondation pour la Recherche Strategique).

Williams. L. E., & Bargh, J. A. 2008. Experiencing physical warmth promotes interpersonal warmth. *Science*, 322: 606-607.

Wilson, Elizabeth J., and Daniel L. Sherrell. 1993. "Source Effects in Communication and Persuasion Research: A Meta-Analysis of Effect Size." *Journal of the Academy of Marketing Science* 21 (2): 101–12. doi:10.1007/BF02894421.

Wohlforth, William C. 2009a. "Unipolarity, Status Competition, and Great Power War." *World Politics* 61 (1): 28–57.

Wood, Graeme. 2015. "What ISIS Really Wants." *The Atlantic*. February 15.

World Bank. 2015. "World Development Report 2015: Mind, Society, and Behavior." Washington, DC. http://www.worldbank.org/en/publication/wdr2015.

Wright, Nicholas D. 2015. "The Biology of Cooperative Decision-Making: Neurobiology to International Relations." In *Handbook of International Negotiation*, edited by Mauro Galluccio, 47–58. Springer International Publishing.

Wright, Robert. 1994. *The Moral Animal: Evolutionary Psychology and Everyday Life* (New York: Pantheon)

Yarhi-Milo, Keren. 2013. "In the Eye of the Beholder: How Leaders and Intelligence Communities Assess the Intentions of Adversaries." *International Security* 38 (1): 7–51. doi:10.1162/ISEC_a_00128.

———. 2014. *Knowing the Adversary: Leaders, Intelligence, and Assessment of Intentions in International Relations*. Princeton University Press.

Zagato, Alessandro (ed). 2015. *The Event of Charlie Hebdo: Imaginaries of Freedom and Control*. Berghahn Press

Zane, N., & Ku, H. 2014. Effects of ethnic match, gender match, acculturation, cultural identity, and face concern on self-disclosure in counseling for Asian Americans. *Asian American Journal of Psychology*. 5 (1): 66–74.