YALE CYBER LEADERSHIP FORUM

Bridging the Divide:

The Law, Technology, and Business of Cyber Security

CONFERENCE REPORT

Edited by Oona Hathaway, Ido Kilovaty, and Ted Wittenstein

APRIL 7–8, 2018
YALE UNIVERSITY, NEW HAVEN

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

We are grateful to the Hewlett Foundation for its support of the Yale cyber security initiative, which has shaped our thinking on bridging the divide between law, policy, and technology on cyber security and thereby made this conference possible. We also are grateful to knowledge partner and supporter, McKinsey & Company, as well as Security Scorecard, Baker McKenzie, Thomas and Mara Lehrman, and an anonymous donor, whose support provided essential scholarship assistance for participants and ensured the success of the Forum.

FOREWORD

After a successful inaugural year, the Yale Cyber Leadership Forum returned in 2018, in collaboration with the Yale Center for Global Legal Challenges and the Yale Office of International Affairs, along with knowledge partner McKinsey & Company. The Forum focused on bridging the divide among the law, technology and business communities in cyber security, and exposing participants to effective approaches to recognizing, preparing for, preventing, and responding to cyber threats. Too often, those with legal, technical, and business expertise do not interact. This has made it difficult to devise effective solutions to the pressing cyber problems.

The team-taught Forum was organized around expert panels, talks by keynote speakers, and small group breakout sessions in which all attendees participated. The Forum drew on lessons learned in a Hewlett Foundation-funded cross-disciplinary course, "The Law and Technology of Cyber Conflict," co-taught by Forum Director Professor Oona Hathaway, along with Professors Joan Feigenbaum and Scott Shapiro. The innovative collaboration between Yale Law School and the Yale Department of Computer Science aimed at spanning the disciplinary gaps between future lawyers and computer scientists, providing a starting point for designing the inter-disciplinary Cyber Leadership Forum conversations.

Now in its second year, the Forum brought together a diverse set of participants, including practitioners from leading law firms, technologists, policy experts, and academics working at the cutting edge of cyber security. (Participants are listed in the appendix to this report.) Every attendee at the conference took an active role in the conversation, and we have made an effort to reflect their contributions here. As with any productive conversation about an issue as challenging as cyber, there was not perfect agreement on any given topic. But the rich conversation generated a number of valuable insights.

This report aims to memorialize the discussion of several key topics of conversation during the Forum. It is not a complete record of proceedings; instead, it provides an overview of four overarching themes of the conference:

- *Cyber risk*, including how to identify and quantify cyber risk, how to manage new risk as a result of the emerging Internet of Things, and how best to ensure basic cyber hygiene to manage cyber risk.
- *Legal and technical tools available to address cyber risk*, including encryption, international law and cooperation, and domestic criminal law enforcement.
- *Business-specific challenges*, including how to develop effective Board-level cyber security knowledge, make responsible cyber investments, develop effective reporting relationships, and nurture executive cyber expertise.
- *Emerging threats,* such as those presented by digitization, big data, and the rise of artificial intelligence; as well as some *possible solutions,* including better education as to risks and how to avoid them, and improving information sharing to better enable criminal law enforcement across borders.

CYBER RISK

Identifying and Quantifying Cyber Risk

The first challenge in managing cyber risk is identifying and quantifying that risk.

Many of the Forum's participants have had experience in quantifying cyber risk as a part of larger operational efforts. All noted that before one can determine how to address cyber risk, it is necessary to understand what the risk might be—in particular, what are the most important assets that might be at risk in a cyber attack.

In order to determine what steps to take to address the risk to these assets, the next step is to decide how to quantify the risk. This is particularly important for those who need to justify cyber security investments by their organizations. The question that one must be prepared to answer, regardless of context (business, government, non-profit), is what steps business should take—how much time and money it should invest—to address the risk. That, in turn, requires not only identifying what is at risk but also quantifying that risk.

The challenge, however, is that there are multiple risk quantification methods. Non-technical assessments, such as expert interviews, are helpful to ascertain potential for impact because business and risk managers need to understand a company's various sources of value in order to determine its vulnerability and potential loss in the event of a cyber attack. This process of risk quantification can help identify the most critical business processes and prioritize the most essential services to preserve or restore in the event of a breach. One Forum participant commented that this aspect of risk quantification is not that much different from the non-cyber Business Continuity Planning that most companies already undertake. Technical assessments, such as passive vulnerability, netflow analysis, or active automated red teaming are necessary to determine the potential likelihood of a breach because probability is largely based on how a technology environment (infrastructure, endpoints, network, etc.) is connected and actually behaves when under attack. In a small group breakout session, Forum participants discussed how every technology environment has grown organically, making non-technical assessments such as a study of architecture diagrams or workflow value chains insufficient to determine the likelihood of cyber attack. The theoretical design of company's IT system is often quite different in practice, and this disparity favors the attacker.

The five primary components of cyber risk quantification: regulatory, productivity, opportunity cost, reputation, and direct financial.

In terms of determining value, the Forum's cyber risk small group landed on five principal components to consider:

- Regulatory – the laws and regulations that mandate certain information security and privacy practices.
- Operational and productivity – how regular business operations will be impacted by cyber risk materializing, including productivity lost due to the psychological state of a workforce.
- Opportunity cost – products and services that are not innovated as a result of cyber risk, as well as attraction and retention of talent.
- Reputation – how the consumers and public at large perceive the company post-breach, which a company can influence by how it responds.
- Direct financial – direct costs associated with cyber risk becoming a reality.


Susan Lander
Yale


EXIT
Yale SCHOOL OF MANAGEMENT
Andrea Maruyshyn

Simplifying cyber risk financial valuation.

The small group discussion of cyber risk observed that it is not necessary to quantify a financial value of risk to decide on a portfolio of initiatives to reduce risk. A simple "high-medium-low" or other non-financial means of quantifying risk, coupled with a technical assessment of likelihood, could get most companies well on their way to productive risk reducing prioritization.

However, the small group agreed there are two very specific use cases in which financial quantification is necessary: 1) using the language of financial returns with senior executives, e.g., to justify budgetary asks or demonstrate the security team's contribution to preserving the value of the enterprise, and 2) to determine levels of cyber insurance.

Ultimately the small group concluded that while some degree of quantification is indeed necessary for prioritization of risk-reducing activities, quantifying that risk in financial terms is not necessarily required. Also, as an agreed-upon methodology for calculating the financial value of risk is not immediately apparent, most companies not requiring either of the two specific use cases mentioned above are likely better served by avoiding cyber risk financial valuation as a part of cyber program construction and prioritization activities.

Internet of Things

The Internet of Things ecosystem increases cyber risk.

The Forum small group discussion of the Internet of Things focused on the dangers and opportunities presented by the emerging ecosystem of the Internet of Things. This is an area of cyber risk that often goes unnoticed, potentially decreasing the barrier on malicious actors. The group considered that topic from three different, yet interrelated, angles.

Industry – the role of Internet of Things manufacturers in controlling the dangers and opportunities of the ecosystem.

Government – the power of regulation and deregulation in mitigating the threats flowing from the Internet of Things

Consumers – individually and collectively, whether consumers can use their leverage to reshape this threat landscape

Countless threats and challenges posed by the "physical Internet".

The small group agreed that the Internet is becoming physical with the advent of the Internet of Things. This creates a host of threats: some are continuations of existing cyber security threats, but others are unique. The small group identified the following primary threats and challenges: *privacy*, *security and safety*, *third-party security*, *scalability*, *dependency*, *evidentiary*, *consent*, and *liability*.

Privacy – ubiquitous sensors brought by the Internet of Things result in mass collection and use of personal data by industry and others.

Security and safety – the exploitability of vulnerabilities and flaws in Internet of Things by malicious actors, potentially resulting in physical consequences.

Third-party security – vulnerable Internet of Things devices exploited en masse to be used as powerful botnets, to target third-party systems.

Scalability – the potential to download entire databases of sensor data at much larger scale.

Dependency – a world without Internet of Things is unimaginable, as society has developed a dependency on the convenience and availability of such devices.

Evidentiary – the legal uncertainty over the collection, use, and retention of sensor data, such as voice and video recordings, for criminal justice purposes.

Consent – the Internet of Things ecosystem collects data about its surroundings, regardless of ownership and consent.

Liability – unresolved allocation of liability for potential materialized harm caused by the Internet of Things.

Medical Internet of Things devices are useful, but certain precautions and procedures need to be followed.

The small group acknowledged that medical devices have a utility when connected to the Internet, but they are also particularly vulnerable. These devices must be designed in a way that puts them on a segregated network. Redundant systems are also advisable to avoid device failure.

Another challenge identified by the small group regarding medical devices is that medical higher education institutions do not train future healthcare professionals for the new reality created by the medical Internet of Things industry. This results in doctors who do not know what questions to ask or how the technology works, potentially harming their future patients.

The advent of what one participant labeled the "Internet of Bodies" makes the problem even more pressing. What began with external, smart objects like FitBits, has steadily grown to Internet-connected pacemakers, microchip implants, and digitized prescription medicine. This "Internet of Bodies" will inevitably expose us to unprecedented cyber security vulnerabilities, introduce conflict across several legal regimes, and raise fundamental ethical questions about the future of what it means to be human.

Externalities and the information gap between consumers and industry.

Several small group participants hold the view that the industry has no obligation to incorporate security until consumers demand it. In another session at the Forum, a speaker suggested that there is already a deep concern among consumers about cyber security, but there does not appear to be a corresponding change in their market behavior. In the absence of market demand for cyber security, vulnerabilities in new products will continue to persist. The lack of consumer demand might stem from information gaps between the industry and consumers.

The group suggested a security rating system that is transparent and allows consumers to make an informed choice. The industry would view such ratings as a competitive advantage, resulting in more secure products. The problem that would persist with such a rating system is externalities imposed by unsecure products. Consumers may decide to purchase unsecure devices because they are less expensive; how do we address the potential harm that decision can impose on third parties? The group agreed that regulation should be the solution in such a context. The group acknowledged that the regular standards that we have been using for rating severity of security vulnerabilities does not map perfectly on Internet of Things questions, and we have to revisit these metrics.

Regulation of Internet of Things is still complicated.

Considering the government's role, the small group agreed that there may need to be a uniform set of standards that applies across industries, given that many problems with Internet of Things are similar across industries. At present, there are critical open questions with regard to overlapping regulatory jurisdictions. The small group concluded that clearer delineation between agencies is necessary for more effective regulation of the Internet of Things.

In that regard, the small group discussed two specific bills introduced in Congress in 2017: 1) The Internet of Things Cybersecurity Improvement Act, and; 2) Security and Privacy in Your Car Act.

The Internet of Things Cyber security Improvement Act Bill (2017) establishes rules to be imposed on contractors who provide Internet of Things devices to federal agencies, requiring verification that these devices do not contain known security vulnerabilities or defects in any hardware, software, or firmware component. The Bill also requires notification, updates (patching), and timely repair.

Similarly, the *Security and Privacy in Your Car Act Bill (2017)* authorizes the National Highway Traffic Safety Administration and the Federal Trade Commission to regulate automotive cyber security. The Bill requires critical software systems to be isolated from noncritical systems, and vehicles to be equipped with built-in systems of detection and mitigation of security breaches.

Many in the group expressed the view that these bills are an important step toward Internet of Things cyber security.

Basic Cyber Hygiene

Most risk is a result of failure to understand and undertake even basic cyber hygiene.

Basic cyber hygiene represents the tools and procedures required to avoid obvious, known, and easy-to-defend against cyber attacks. The difficulty, however, is that the vast majority of those using connected devices have little to no understanding of even basic cyber hygiene. Even students interested in cyber policy and law often lack basic technical expertise. Educators often have to teach cyber security to students from non-technical fields. These students are likely to lack the essential experience and knowledge of how computers, networks, and hacking works. This represents a serious obstacle for the effective teaching of cyber security-related courses, and requires that educators first focus on the technical basics before moving to cover the policy aspects of cyber security.

The Forum included a live demonstration of some basic cyber exploitations that highlight common cyber risks—many of which can be easily defended against using common sense cyber hygiene.

The risk of inconvenience.

A zip-bomb attack represents an attack that could pose an inconvenience to its victim through unintended effects. This attack involves the creation of a zip file with a small payload and a large, empty file to make the zip file appear full. The attacker then uploads the zip file to a semi-anonymous file-sharing site and sends an e-mail with the download link to the victim. When the victim downloads and unzips the zip file, it fills their file system with "junk" files which they must go through and manually delete. Compared to other attacks, this attack mainly causes inconvenience; yet it is a risk that is easily preventable by not opening unknown attachments.

Unauthorized access and remote command execution.

A malicious user can do more than simply irritate his or her victim. For example, misconfigured privileges could cause far greater damage than inconvenience. It is not uncommon for a website to include a ".config" file that contains plaintext login information for databases underlying the website. In a well-configured website, the owner of the site has read and write access to this file, the administrators have read-only access, and visitors to the site have no access. A negligent system administrator, however, may back this .config file up and forget to restrict the permissions on the backup file. Malicious actors could use their knowledge of common practices to look for files with misconfigured privileges. Finding this backup .config file could allow them access to the backend of the website and export the database underlying the website. Attackers could also change the password to their own, which would allow them to edit and deface the website.

The website would log any of these attacks, so a sophisticated attacker would disguise his identity, location, and what was stolen by using a Tor browser. Tor routes a user's traffic through several nodes (onion routing), so a Tor user in New Haven could appear to be located in Romania. Additionally, Tor allows a user to access certain ".onion" websites, which are not accessible using regular browsers. These websites are often referred to as "the dark web." Pairing Tor with tools like OnionShare—a filesharing service on the dark web[1]—empowers malicious actors (but also political activists and journalists) to anonymously share data which has been stolen. The victim of this attack, therefore, would not know what was stolen and the attacker could appear to be located anywhere in the world.

Unauthorized access to sensitive data is not the end of the story. Malicious actors can also execute commands remotely by conducting an XSS (cross-site scripting) attack. Websites which accept user inputs can, in some cases, allow users to insert commands into the site through those inputs. A user could insert an instruction into a form which adds fields into the form (which the attacker could intercept using a man-in-the-middle attack), changes the text of the site, embeds another website, pastes in an image, loads malicious scripts, or delivers a file payload. This instruction, for many sites, would be added to the end of the URL. It is easy for companies to protect against XSS attacks—sanitizing inputs only requires a single line of code—but many do not. This is just one example of how basic cyber hygiene methods are not always followed and create systemic vulnerabilities as a result.

Eavesdropping could be software- but also hardware-enabled.

While malware could eavesdrop on a user, hardware and hardware-based vulnerabilities are becoming increasingly popular for surveillance attacks. One example of a hardware-based vulnerability is *Spectre*, allowing a speculative execution attack. Last year, researchers discovered a critical vulnerability in Intel processors, which allows attacks to peer into cache memory and use microprocessors' speculative execution functions to access data belonging to other users. In this attack, they targeted a web server providing cloud hosting for a form. They had a member of the audience submit a secret message through that form. This exploit first runs a script to check whether the targeted machine has an unpatched firmware, making it vulnerable to the *Spectre* and *Meltdown* attacks.

Because the server did have those vulnerabilities, the attacker was then able to read through the cache memory to find the secret message. There are patches now for these vulnerabilities, but this exploit demonstrates that it is possible to violate the constitutional principle of networks: separation of users.

Staging a man-in-the-middle attack is also relatively easy using specific hardware. Raspberry Pi, a thumb-drive size router, runs a "rogue" wireless network connected to another, legitimate network. The victim would connect to the rogue network, which asks the user to download a malicious certificate. Most users are used to facing similar prompts while using public WiFi networks and would agree to download the certificate. The Pi network is now able to intercept and (using that certificate) decrypt the victim's communications. Even if a connection appears secure, such as when logging in to an e-mail service, the Pi network could still intercept and decrypt the communications, while also collecting the username and the password.

These basic attacks demonstrate two serious challenges. First, that cyber security education often neglects addressing these basic, yet potentially devastating, attacks. Second, that cyber risk should account for basic cyber attacks, just as it would with more advanced threats.

[1] The dark web is a set of websites which users can only access through a Tor browser. Users can use it for legal or societally beneficial ends (securely passing information to journalists) or harmful ends (illegal markets).

LEGAL AND TECHNICAL TOOLS TO ADDRESS CYBER RISK

Encryption

Encryption is not a panacea, but it is an important tool.

Many of the recent security incidents were enabled by unauthorized access to plaintext data. Encrypting such data could have prevented these incidents from happening. One of the Forum's speakers argued that encryption is being underutilized by vulnerable sectors, such as federal government agencies, who constantly seek to develop unnecessary new technologies to preserve privacy and security. According to that speaker, while existing technologies would be effective at protecting users, users have not adopted them on a wide scale.

Good security and privacy technologies have existed for a long time, but the real challenge is getting decisionmakers and consumers to use these technologies. There is some progress on this front: for example, certain insurance companies offer discounts to companies that protect their data well and refuse to insure companies that do not take adequate steps to protect their data. Additionally, users have also started to recognize the importance of security and privacy. The way forward is to create more security software designed to be trivial to use, so that users will not have to think as much about security.

E-commerce is an example of such successful implementation: most e-commerce is protected by strong encryption, and users do not have to think or learn about implementing that encryption.

This reality has also led to an emerging phenomenon of "technological unilateralism," where tech companies make devices that they do not have the technical capacity to unlock. They give consumers the ability to set their own security and say that any disputes over information access should be between the government and users.

There is a tension between strong encryption and law enforcement access.

Law enforcement agencies regularly dispute the practice of technological unilateralism, contending that their ability to access vital evidence for criminal-related and national security investigations is significantly diminished as a result. One Forum speaker sees this debate as having both technological and policy aspects. The technological question is whether it is possible for hardware and software makers to grant law enforcement access to encrypted devices without compromising the encryption in other cases. The policy question is whether they *should*.

Indeed, yet another speaker at the Forum highlighted that law enforcement's access to metadata is not sufficient for effective criminal investigations. While metadata is valuable in certain situations, it often lacks the operational details pertaining to terrorist attacks: the target's identity, method of attack, or the timing of the attack. This speaker believes that lawful access to encrypted data is technically possible without compromising the overall security of the encryption. This could be achieved in the same way that hardware and software manufacturers access decrypted data, through an update channel in their product that allows them to add features and fix bugs. Granting law enforcement such power would not weaken security.

According to this speaker, market and commercial enterprise should not be the deciding vote. The framework proposing government access to plaintext published by the National Academy of Sciences should provide a sound basis for a potential solution. That solution should follow a national discussion involving technologists, academics, national security professionals, law enforcement, privacy and civil liberties advocates, and other relevant parties. Eventually, Congress will have to enact legislation which draws a clear line between absolute data security and national security. That is the trajectory for encryption.


John Evangelakos
Sullivan & Cromwell
Valerie Feldmann
Palestrina Group


Yale Cyber Leadership Forum
Joan
Feigenbaum
Yale University


Blumetti
Classroom
Welcome to the
Yale
Cyber
Leadership
Forum
Yale University
New Haven, Connecticut

Participants agreed that the government should ensure the availability of strong encryption to its citizens to the extent possible. A key area of contention is whether exceptional law enforcement access is technologically possible, and if so, whether such policy would be wise to adopt.

Nevertheless, encryption and other security and privacy technologies cannot solve all cyber security problems. Russian election hacking and the Cambridge Analytica scandal represent failures of policies—not technologies. The wrongdoing in these cases was fraud, not hacking. There are no technological solutions for this abuse of technology by foreign adversaries, tech companies, and platforms.

International Law

International law could mitigate transnational cyber threats.

The Forum explored international law as a potential solution for transnational cyber threats. A speaker introduced the basic tenets of international law as it applies to cyber space, and later on, a small group dedicated to the topic continued the conversation.

The speaker introduced the topic by discussing three basic questions that international law seeks to answer: what actions is a state prohibited from undertaking in cyber space? What are states allowed to do? And what obligations does a state have to prevent harm to another state?

The use of cyber force is strictly regulated by international law.

The U.N. Charter Article 2(4) is the law governing use of force, including activities in cyber space that reach the level of "force." It reads:

> *"[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."*

There are three exceptions to the above prohibition on the use of force: (1) authorization from the UN Security Council; (2) consent from the target state; and (3) self-defense (or collective self-defense) pursuant to Article 51 of the UN Charter.

Most cyber attacks are not severe enough to reach the threshold of Article 2(4)'s prohibition on the "use of force." Even fewer meet Article 51's requirement of an "armed attack." For example, the Stuxnet worm that infected Iranian nuclear research facilities was arguably a "use of force," but not an "armed attack." Also, the Sony attack probably not even a "use of force," but close.

The situation is complicated by the fact that the U.S. government has taken the position that the prohibition on the "use of force" in Article 2(4) is the same as an "armed attack" that gives a right of self-defense in Article 51. This approach leads to a potential escalation, since more cyber attacks would entitle the victim to respond in self-defense.

If cyber attacks do in fact reach the level of a use of force and armed attack, there is a whole other body of international law that needs to be taken into account: the law of armed conflict, which governs belligerents' behaviors during war, limiting what cyber tools may be used in times of war. The two key principles mandated by the law of armed conflict are distinction and proportionality, which are difficult to apply to the cyber realm.

International law does not always fit to the realities of cyber security. Certain initiatives – such as the *Tallinn Manual* – are attempting to clarify the law.

The leading work on the international law applicable to cyber operations, the *Tallinn Manual 2.0*, focuses on what it calls violations of "sovereignty." Rule 20 of the Manual states that, "A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that is owed by another state."

There are several limitations on countermeasures. They can only be taken in response to an internationally wrongful act; they must be proportional to the injury; they may only be taken by the state that was harmed; and their purpose must only be to induce a state to comply with its legal obligations. Once the internationally wrongful act has ceased, they may not be used anymore.

As to the definition of "internationally wrongful act," the *Tallinn Manual* 2.0 answer is "violation of sovereignty." It defines sovereignty as: "independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other state, the functions of a State." But this applies an exclusively territorial model to cyber space, which creates a shaky analogy where the limits of sovereignty are not clearly delineated. For example, would the Voice of America be in violation of sovereignty?

The *Manual* also says that a state "must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other states." The concept of due diligence is clearly important, but it provides no specific guidance as to what states are obligated to do.

International law enforcement is available to states, even when a cyber attack does not reach the level of "force" or "armed attack".

Forum participants were interested in the enforcement tools for international law violations. The speaker presented a variety of avenues in response to cyber attacks that violate international law. First, economic sanctions are an example of a legal mechanism that can be used in response to violations. On the other hand, retaliation—so called "active defense"—ought to represent a much more limited tool. The *Tallinn Manual* approach is that lack of cyber deterrence encourages more attacks; therefore, designating a violation of sovereignty by cyber means as an illegal act could authorize countermeasures in response. However, there is a concern that this approach would authorize a large range of active responses. Moreover, the concept of "sovereignty" put forward in the *Manual* is not widely accepted as a legal basis of countermeasures.

Cyber deterrence through due diligence, criminal prosecution and indictments, and outcasting.

One speaker suggested that when government is either not able or not willing to defend them, perhaps such actors should be permitted to engage in active defense for themselves (actions which are admittedly currently unlawful under domestic law). It was pointed out that while there may not be force involved, the stealing of, for example, weapons technology, can have security consequences. The rest of the group felt this was not a productive approach, as it can lead to tit-for-tat attacks that put private companies in an impossible situation.

The international law small group considered three alternatives to self-defense and to "active defense" by government.

(1) Due Diligence. International law mandates a due diligence requirement, which requires states to prevent transboundary harm by all feasibly reasonable means. The small group acknowledged that the U.S. is the largest source and destination of attacks because the U.S. has the largest telecom infrastructure. It is believed that for that reason, the U.S. has been reluctant to adopt a due diligence requirement as advocated by the *Tallinn Manual*.

(2) Criminal Prosecutions and Indictments. Several small group participants highlighted the potential of indictment of individuals. There are rules, and many states know what they are. Domestic criminal law can be used as a key tool for enforcing them. This entails enforcement on a sovereign basis, through domestic legal authorities. While some countries are better at enforcing their laws, this tool can also be effective for those countries that will not cooperate, or whose rule of law concept is shaky, because an indictment could impose serious restriction on such individuals. For example, those indicted cannot travel for fear of being turned over. A number of these tools have been used very effectively in the terrorism context, for example. And mutual legal assistance treaties can sometimes be used to get ahold of actors abroad.

In the U.S., when the election hack was happening, domestic authorities were much quicker to respond after the election infrastructure was designated as critical infrastructure. That kind of decision can make a large difference in activating criminal law authorities, like the FBI, to respond more quickly and aggressively. The small group was at near-consensus that the domestic enforcement model works for criminal law issues.

(3) Outcasting. International exclusion and other forms of sanctions to enforce cyber laws. For example, if a nation-state is stealing a patent or trade secret to advance its own private sector, such state could face consequences. If enough evidence of such conduct is presented to the U.S. Department of the Treasury, then that nation could face exclusion from the U.S. sector with which the intellectual property is associated. Subsequently, this intel could also be shared with close allies (Five Eyes), encouraging them to pursue a similar course of action.

In the past, the U.S. did bring patent and trade secret litigation where cyber theft was involved, for instance in cases involving DuPont and Chevron. While DuPont had spent large amounts in China on building a plant and, when China stole this technology, DuPont responded by pulling out of China, Chevron did not have that option available because China is too large a market for it. Outcasting, therefore, works for certain actors but not for others. The small group agreed that thinking in terms of carrots and sticks for granting/limiting access to markets/clubs (unilaterally or multilaterally) is helpful.

Do concerns about setting international legal precedent foster inaction and erode deterrence?

Some speakers and participants expressed concern that the U.S. government has proved unwilling to impose meaningful costs on its adversaries for engaging in malicious cyber activity. In order to encourage a stronger and more effective response, it is possible that criminal prosecutions, indictments, targeted sanctions, or outcasting may be insufficient in certain cases. One possible suggestion is to consider more aggressive U.S. use of offensive cyber tools to degrade an opponent's ability to attack.

Discussion ensued regarding whether an offensive U.S. cyber campaign would be legal under international law, and whether it would contravene fundamental values. Some speakers and participants noted that state actors such as Russia and Iran have escalated their own cyber operations, even without the U.S. engaging in offensive operations, out of fear of setting a precedent. In fact, some assert that U.S. reticence to launch a cyber offensive of this sort may be emboldening adversaries and inviting even more malicious cyber behavior. One participant highlighted options such as sanctions and indictments, which should be exhausted before exploring more aggressive actions. The challenge, however, is that the message being sent by sanctions may not currently be heard, since many countries continue to engage in cyber operations against the United States.

Law Enforcement

U.S. law enforcement may deter cyber crime, especially through private-public partnerships, but there are challenges.

Forum participants also focused on the myriad challenges that law enforcement authorities face when investigating cyber crime, or when attempting to access digital evidence related to criminal activity.

One recurring example of the so-called "Going Dark" challenge is the locked iPhone belonging to the terrorist in the San Bernardino attack of 2015. To address rampant thefts of iPhones and theft of personal data, Apple started to use encryption across the board to protect user data. Such practice immediately raised an important question on the government side – can law enforcement get in? The San Bernardino case shows that law enforcement can eventually circumvent locked devices, if sufficient time and resources are used. The Department of Justice Inspector General Report noted that: "an outside party had demonstrated to the FBI a possible method for unlocking the iPhone… the FBI had successfully accessed the iPhone and no longer required assistance from Apple."

One speaker at the Forum, arguing in favor of end-to-end encryption and against exceptional law enforcement access, claimed that this third-party method of breaking into devices is an important tool for law enforcement to have. And while it is expensive to hire outside assistance in breaking locked devices, it is no different than other law enforcement methods such as wiretaps. This conclusion should strengthen the case for unbreakable encryption without exceptional law enforcement access.

Strict and transparent legal procedure should govern exceptional access.

The Forum's cyber crime and surveillance small group focused its discussion, among other things, on how to avoid abuse of access should exceptional access to decrypted data become a reality. The small group participants pointed out that there are legal frameworks, procedures, and tools to access data as needed, but that these must be used in a structured and legal manner. While many do not agree that Apple should give up its source code, there is a tension with the need for cooperation with law enforcement to protect against security incidents. In the intelligence community, there is education and auditing to prevent the abuse of power. There are many control features in place to prevent abuse.

Transparency is crucial. Even if consensus is reached about a process, analysts still need to provide factual information to set expectations. Certain participants suggested that the term "backdoor" would be misleading in that context. If we create a known legal process to access encrypted information, we should be labeling that as "decryption warrant."

There is the assumption that law enforcement going through the front door would necessarily mean abuse from the back door, so malicious actors would be able to access such information in the same way. There are potential unexplored technological solutions to such concern – e.g. "single use key" – which would also control market risks, and ensure customers trust the company in question.

The small group participants noted that looking through smartphone files is often thought of as analogous to people looking through physical files in the analog days. The difference here is that there is an unreasonable expectation of privacy today. People assume that their devices are more secure than their homes. But people think this because they think of their phones as an extension of their minds; smartphones are repositories of our information and preference. In the mind, there's a functional relationship between belief and desires. A smartphone does similar things by suggesting what its user might like, becoming an extension of one's mind. However, this might be a reasonable expectation because it might be possible to make the phone more secure than the home. The privacy discussion could be a positive tradeoff, given generational differences in approaches to privacy.

Private companies which assist the government though private-public partnership are not bound by the same laws, but perhaps they should be.

Indeed, private tech companies are not bound by the same laws as the government. For example, a tech company representative in the small group indicated that law enforcement is not involved in their investigations unless it's complete. There are already controls within the private sector; the biggest control is public perception. If a private tech company is too close to law enforcement, it is often perceived as bad for business.

Public-private cooperation involves many actors within the government and outside of it. The military and the Department of Homeland Security have a set of capabilities and relationships with defense contractors, and there are a wide range of ways a private company could assist different public entities. For example, if Apple's next phone was designed so that there were decryption keys obtainable with a warrant, it would mean that Apple would be involved in a long-term process that assists law enforcement. If we go this route, these public law values (transparency, fairness, due process, accountability) should bind private-public partnerships.

But there is a difference between law enforcement and intelligence. In order for law enforcement to use this intelligence, they must follow these procedures. But intelligence entities don't need to. The same public law values should bind the government and private companies; otherwise the government could just outsource certain problematic tasks to private companies, knowing that they would not be held to the same standard.

The difficulty of attribution in cyber space is a serious obstacle for law enforcement.

Attribution is a major challenge in taking action against malicious actors. The FBI, Interpol, tech companies, and many others are trying to find the "sweet spot" between attribution and responding to security incidents. A prominent tech company representative participating in the Forum admitted that their company is working on protecting its customers, which include many banks and other critical infrastructure, and it is therefore crucial to respond in time.

A problem that arises from that company's need to protect its customers is that such protective operations often collide with ongoing law enforcement operations. Cooperating with law enforcement authorities is therefore essential to preventing these collisions.

A few open big questions include: what weight does attribution need to accumulate before the eventual arrest? How quickly should the harm be eliminated? How can we address jurisdictions that do not have extradition treaties with the US?

Another speaker at the Forum suggested that attribution is chiefly important for law enforcement, while for the private sector the emphasis should be on protection. Whereas law enforcement's first question should be "who's doing it?" the private sector should be asking "how do I get back up and running properly?"


Sean

BUSINESS-SPECIFIC CHALLENGES

Sophisticated firms appreciate the cyber threat, and their investments in cyber security are on the rise.

Forum speakers observed that sophisticated firms and their corporate boards now are fully aware of the threat that cyber security poses to business, but it has taken time to grasp the scale of this challenge, and many preventable breaches have occurred in the interim. Even a decade ago, major financial firms did not invest sufficiently in cyber security and lacked an understanding of the cyber security threat from sophisticated state actors, primarily China. Yet especially in the past five years, Forum speakers and participants observed a growing investment in cyber security and recognition of the need to retain cyber expertise. One speaker estimated that, in his experience, major companies now need to spend between 3 and 10-percent of their revenue on cyber security—and that closer to 10-percent often was necessary.

Sophisticated financial firms and major companies in other sectors now prioritize hiring the very best former government cyber experts available in the private sector, to include top research and data scientists from the U.S. intelligence community. Successful companies increasingly view cyber security as a valuable investment as opposed to a sunk cost. Although it is a significant expense, cyber security efforts – especially data compliance and identity verification measures – have the potential to create efficiency and productivity gains. The benefit of these precautions is that they force companies to focus on what data they have, and where it is located.

Yet even sophisticated firms still do not invest wisely in cyber security, creating persistent vulnerabilities due to waste, inefficiency, and lack of investment in human training vs. technical solutions.

Even when firms have the ability to absorb significant cyber security expenses, speakers and participants alike expressed concern that the budgets of most firms are greatly misguided. One speaker assessed that companies tend to invest about 80-percent of their cyber security spending in reactive technologies, which detect an irregularity after it occurs, but only stop about 3-percent of attacks. Companies then invest the remaining 20-percent in proactive technologies, which can identify system weaknesses and respond to potential threats that have not fully materialized, but even those technologies often can stop only up to 45-percent of attacks. A core challenge is to convince firms to be more proactive in terms of how they invest in cyber security solutions.

Moreover, the cyber security marketplace is inundated with companies offering false or misleading magic solutions. Even major companies often falsely believe that the technology investment itself is sufficient, but fail to integrate it properly into business operations through regular interaction and human training. Expensive cyber technologies often are ineffective absent rigorous human training, and companies often learn this the hard way through preventable cyber attacks.

Less sophisticated and smaller firms lack detailed cyber knowledge and the capacity to invest in cyber security, generating even greater business risk.

Forum participants expressed concern that only the largest and most sophisticated companies can afford effective cyber prevention and response capabilities. Cyber security is the fastest growing market domestically and globally; this year about $7 billion in venture capital went to financing new cyber companies. But these investments predominantly go to larger cyber security companies, and about a dozen U.S. companies control large shares of this overall investment. Moreover, these services only are affordable by a small number of highly successful companies.

As a result, significant vulnerabilities persist in small and medium-sized businesses. Yet given the nature of global commerce, cyber attacks on these businesses can have a disproportionate effect on consumers, as well as impact major companies that rely on smaller ones as part of their supply chain.

Board-level knowledge of cyber security is crucial, but there is an executive talent gap and no "one-size-fits-all" approach; each company must decide the proper reporting relationships.

Participants agreed that any corporation's operations division must fully integrate IT, cyber security, and other technologies into a company's overall business plan. One speaker observed that a Board must be involved in the broader structural challenges and strategic investments associated with cyber security, but detailed threat knowledge is an unrealistic expectation. The challenge is how to bridge the technology-business divide in terms of cyber knowledge within a firm, especially at a company's highest levels. There is no easy solution to this problem, but it requires constant attention and regular interaction at the level of firm leadership.

Before determining an organizational structure, companies must identify their own information security requirements, organizational design principles, and reporting requirements. Incorporating chief information security officers (CISO) into C-suite and Board-level discussions, for example, prepares information security executives to prioritize efforts in a way that make sense for the business, limiting risk when done well.

Nationally there is a shortage of CISO leadership that decreases security, increases risk, and impairs assessment efforts. The talent gap among CISOs is real: projections suggest more than one million critical information security-related roles will be unfilled in North America over the next 2-3 years. CISOs routinely grapple with this challenge, as well as where and how to report within their organizations.

But organizing to manage cyber risk is not just about talent and organization. Mitigating real risk of value destruction also requires: designing and executing a program of controls to identify, protect, detect, and respond to threats in areas of highest value at risk; securing not just the right level of cyber insurance policy but also lining up third parties on retainer to augment enterprise capabilities where in-house capabilities to remediate and recover are lowest; and driving more strategic conversations with the firm about why, where, and how to improve business-side understanding of cyber culture and awareness.

EMERGING THREATS

The cyber threat landscape is constantly changing. Certain technological trends may soon materialize into concrete dangers.

The Forum covered a host of future challenges to cyber security, which could reshape the threat landscape, and as a result, our tools of addressing security challenges. Trends in digitization and big data, artificial intelligence, and eroding boundaries give insight into what the future of cyber security challenges might look like.

Digitization and Big Data

The scope of data collected about us calls for regulation that focuses on the use of such data, rather than its source.

Big data is comprised of ubiquitous data about individuals, both voluntary and involuntary. The volume of data produced daily is astronomical. Every minute, Amazon makes over $250,000 in sales, 103 million spam emails are sent, Google conducts 3.6 million searches, 15.2 million texts get sent, and Snapchat users share 527,000 photos. We produce 2.5 quintillion bytes of data per day, according to IBM. Put another way, that's 2.5 exabytes of data each day (around 2.5 billion gigabytes).

Some of that data is voluntarily given away when users sign up for services or applications. Users rarely read the 32-paragraph end user license agreement or notice that in paragraph 27 they waive all rights to data about their habits, location, browser history, and so forth.

The existence of some data about users is not even known to them. This includes data collected by license plate scanners, security cameras, grocery store scanners, and others. But it produces data about people and what they do. What could an unscrupulous party do with that kind of information?

Every technology can be used for both good and evil. The combination of the Internet of Things – connected devices like Internet connected cameras, thermostats, doorbells, refrigerators, and sensors – and data science means that the number of sources and volume of data are going to increase by orders of magnitude. The Internet of Things small group reached a similar conclusion, emphasizing that the Internet of Things industry creates broad and unnecessary databases with sensitive information collected by sensors.

A Forum speaker argued that our current construct for managing this is a small data approach. We rely on laws that govern how the data is acquired – the informed consent model of EULAs, or the legal acquisition by the government or corporations. But that approach ignores the fact that we are surrounded by an ever-increasing set of data sources.

Instead, as one speaker suggests, we should look at a construct that focuses on the uses of big data, one that governs what is done with the data, regardless of its source.

With digitization, data is becoming easier to steal and manipulate.

Another Forum speaker pointed out that digitization means that almost everything is scanned and stored online, inevitably making it easier to steal through cyber theft. Even the most valuable data is becoming harder and harder to protect, given that sophisticated malware has proliferated, and it is available to attackers at cheaper and cheaper cost.


Yale Cyber Leadership Forum
Yale Cyber Leadership Forum
Sean

Another Forum speaker argued that cyber security threats were initially considered through the narrow lens of cyber crime—i.e., theft of data. New concerns focus on data manipulation and alteration. Threats from voice recognition, voice impersonation, and video manipulation will make identity verification even harder in the future.

Artificial Intelligence

Artificial intelligence may improve cyber security, but it could also create new vulnerability.

A Forum speaker claimed that certain types of automation, which are sometimes referred to as "machine learning" rather than "artificial intelligence," do suggest the possibility of rapid vulnerability detection and response—at least for all but the most sophisticated types of cyber attacks.

Another speaker concurred, arguing that artificial intelligence needs to become an integral part of any future cyber security plan. Artificial intelligence has great potential to help with detecting vulnerabilities and processing vast amounts of threat data. Although the technology is not yet fully realized, national-level attention can ensure that artificial intelligence becomes more of a cyber security opportunity than a threat.

A third speaker was more skeptical, noting that automation had an equal chance of increasing cyber security vulnerabilities. It used to be that there were mainly two types of cyber attacks: long-term attacks that were specific and hard to defend; and broad-based, crude attacks. However, automation creates the possibility of mass cyber attacks that are both broad and hard to defend, specifically tailored to particular industries or types of data.

Solutions

Forum speakers and participants provided some insights on potential solutions to future cyber security challenges.

Zero Trust. Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its IT perimeters, and instead must verify anything and everything trying to connect to its systems before granting access. The strategy revolves around cutting off all access until the network knows who you are, and not allowing any access to IP addresses or machines until it is confirmed that a user is authorized. This speaker is optimistic that this mentality is starting to take place in many firms, and new technologies are coming to market that can help implement such a strategy.

Education and bridging the gaps. Throughout the Forum, many speakers highlighted the lack of expertise among public officials, as well as the gaps between security experts and policymakers. A speaker explained that regulators and computer scientists lack a shared language for discussing cyber security. Security and privacy are two different technical concepts, but policymakers have been slow to grasp and react to this challenge. Another speaker explained that the lack of public sector expertise was a significant challenge, with levels of expertise widely varying across agencies, making cross-agency conversations difficult. When discussions lack detailed technical expertise, there also can be a risk of over-bureaucratic conversations that bias against action.

Better outcasting tools. The United States could do more to condition access to its markets and cyber security infrastructure on good behavior—both for private companies and foreign states. This is a tool that companies can employ on their own, as well, refusing to do business or share information with actors that fail to abide by certain cyber norms.

Better law enforcement cooperation across the divide. Private companies and government sometimes find themselves at odds when it comes to law enforcement—witness the battle over backdoor access. But some companies have found productive ways to work with government around cyber security issues, not only in the United States, but around the world. Many governments lack expertise to build cases against cyber criminals in their countries; meanwhile private companies have few tools for penalizing actors using their products or networks for nefarious purposes. The two can work more effectively in tandem—with private companies producing data and sharing it with law enforcement authorities that are then able to take malicious actors into custody and prosecute them effectively.

Building CISO executive talent and board-level cyber expertise. While sophisticated firms appreciate the cyber threat and investments in cyber security are on the rise, gaps in expertise and vulnerabilities still persist, especially for smaller and medium sized businesses. The national CISO shortage requires a dedicated strategy for education and training. Although Board-level cyber knowledge is on the rise, in-depth attention to cyber security reporting relationships is essential and there is no "one-size-fits-all" approach.

PARTICIPANTS[2]

Sarah Baker, Healthcare Ready
Drew Bartkiewicz, SignID
Eric Benninghoff, Yale University
Austin Berglas, BlueVoyant
Jim Boehm, McKinsey & Company
Richard Boscovich, Microsoft
Aaron Bradley, 41st Intelligence Squadron USAF
Jacqueline (Lyn) Brown, FBI
Joseph Burson, Yale Law School
Jonathan Cardenas, Yale Law School
Jasson Casey, SecurityScorecard
Emmett Cassidy, Yale University
Leila Chang, Yale University
Claude-Yves Charron, Université du Québec à Montréal
Betsy Cooper, UC Berkeley
Nicholas Curcio, McKinsey & Company
Andrea de Sá, Yale Law School
John Evangelakos, Sullivan & Cromwell
Joan Feigenbaum, Yale University
Valerie Feldmann, Palestrina Group
Axel Gonzalez , 41st Intelligence Squadron USAF
Andrew Grass, McKinsey & Company
Oona Hathaway, Yale Law School
Dorothy Hill, Pallas Global Advisors
Fred Hintermister,NERC E-ISAC
Claire Kalikman, Yale Univeristy
James Kaplan, McKinsey & Company
Elsie Kenyon, Nara Logics
Ferdous Khan, Northrop Grumman
Ido Kilovaty, Yale Law School
Elena Kvochko, Financial Services sector
Susan Landau, Tufts University
David Lashway, Baker & McKenzie
Richard Ledgett, National Security Agency (fmr)
Richard Lethin, Reservoir Labs / Yale University
Charlie Lewis, McKinsey & Company
Marina London, Employee Assistance Professionals Assoc.
Ron Lubash, Cycurity
Ji Ma, Yale Law School
Kenneth Mackiewicz, Sovereign Intelligence
Bret Martin, H3 Biomedicine
Andrea Matwyshyn, Northeastern University
Micaela McMurrough, Covington & Burling
Thomas Moore, 41st Intelligence Squadron USAF
Sean O'Brien, Yale University
Dan Omohundro, 41st Intelligence Squadron USAF
Leslie Powell, Yale University
Asha Rangappa, Yale University
James Rosenthal, BlueVoyant
Eric Rubenstein, Image Insight Inc.
Dan Schmechel, Ecolab
Andrea Sehl, Bulldog Innovation Group
Willie Session, HSBC Bank
Scott Shapiro, Yale Law School
Daniel Sislo, United States Air Force
Marc Sorel, McKinsey & Company
Matthew Spence, Guggenheim Partners
James Stranko, McKinsey & Company
Michael Sulmeyer, Harvard University
Nancy Sumption, MITRE Corporation
Brett Warrick, Sensato
Arnold Webster, Army Cyber Command
Zoe Weinberg , Yale Law School
Edward Wittenstein, Yale University
Hannah Wood, Yale University
John Woods, Jr., Baker & McKenzie
Tian Tian Xin, Yale Law School
Aleksandr Yampolskiy, Security Scorecard
Claire Zalla, Yale University
Jennifer Zuccaro, Yale University

[2] Affiliation provided for identification purposes only; participants participated in the Forum in their personal capacity.