DIGITAL BORDERS AND ASSETS IN NATIONAL CYBER RESILIENCE

FEBRUARY 2023

Authored by: Ollie Whitehouse

BinaryFirefly

Think Tank Report

BinaryFirefly

Vision and Mission

Established with a vision for a boutique organisation that serves the needs of a small family of handpicked interests which in turn enables us to serve society.

Our mission is to provide clearly differentiated quality and value in what we do in the domain of cyber.

Our edge is built on over 25 years of experience in cyber defence and offence. Working across directorships, investment, strategy, operations, research & engineering.

Operating boardroom to binary to enable cyber objectives in an ever-changing world through research, analysis, insight and capability.

email: hello@binaryfirefly.com
web: https://www.binaryfirefly.com/
twitter: https://twitter.com/binaryfirefly

Contents

National Digital Borders and Assets

Preface

Governments produce quantified comparators both with itself and others often periodically to show progress against stated policy objectives. We suggest that for Governments to be effective in their cyber resilience objectives they need to be able to define where their digital borders begin and end as well those digital assets which comprise their national asset register both in and out of country across Government, Academia and the Private Sector.

In the context of cyber risk, the assets that comprise a country can be seen as analogous to the assets that comprise an organisation. Being able to define and identify such assets is considered a fundamental requirement to cyber hygiene in contemporary governance. Similarly there have been calls and proposals for the US to have a Bureau of Cyber Statistics and the UK to have an Office of National Statistics of Cyber. We suggest for such organisations to be effective would similarly require definition and identification of assets.

This paper explores the considerations around how the digital borders and assets that comprise a country may be defined.

Challenge

Where do national digital borders in a digital/Internet era begin and end? Can a country's national digital assets and those of its organisations exist outside of its national digital borders?

For Governments these are questions they will seek to answer as they look to define and assess:

- Sovereignty
- Critical National Infrastructure
- Levels of risk arising from National Attack Surface, Vulnerability and Threat

We suggest that without defining the assets a country considers its own responsibility (sovereign) versus those it is reliant on others to protect it cannot accurately assess, quantify nor manage its associated risks in contemporary national cyber resilience.

Digital Borders and Assets

In the physical world national borders are a concept which have long been understood and enshrined in various international constructs, laws, treaties and agreements. In the digital world such concepts we suggest are today nascent and opaque.

Country Addressing: Address space which routes digital traffic to a country
The digital assets which enable the electronic routing into a country's physical borders for service are likely the easiest to define and understand as both comprising a country's digital boarders whilst being considered a digital asset.

In the context of telecommunications and the Internet these would include radio frequency spectrum, telecommunications signalling global title routing and IPv4/IPv6 address spaces that result in digital traffic entering networks physically located within the country.

Country Assigned: Assets assigned to a country
The digital assets which are assigned to a country by international agreement or governing body are similarly easy to conceptualise as being considered digital assets that belong to a country. However, whether or not systems serving these assets fall within a country's digital borders cannot be guaranteed thus raising various questions around sovereignty.

Examples of such assets include telephone country codes (e.g. +44, +61, +65, +81) and country top level DNS domains (e.g. .uk , .au , .sg, .jp etc.).

Country Hosted: Assets running inside of a country
Digitals assets which run within the physical borders of the country, be they physical, virtual or logical and comprised of networks, hosts and services are easily understood to be within country and thus sovereign.

Country Controlled: Assets run by an organisation headquartered or subsidiary located in country
Opaque are those digital assets which comprise the digital estates/environments of organisations which are either headquartered or are a local subsidiary located within a country. Be the organisation government, academia or the private sector.

These digital assets may or may not entirely operate within the country's physical borders due to the advent or modern computing paradigms such as cloud, software-as-a-service and the globalisation of supply.

These assets may be physical, virtual or logical across networks, hosts and services whilst being potentially globally distributed. However, the existence, loss or compromise of these assets presents a potential risk to the organisation and thus by proxy the country.

Equally who owns and/or is responsible for the asset at a physical, virtual or logical level may likely vary across complex supply chains. Where the asset exists physically may also be distinct from the various owners or responsible entities.

Yet when a country wishes to define those digital assets which comprise critical national infrastructure in order to assess and measure risk complexity arises. We assert that achieving understanding is critical in order to assess and quantify the national attack surface, vulnerability or threat.

Country Critical: Assets which are critical to the functioning of a country
Finally, there are those assets which are critical to the functioning of a country irrespective of where they are located and who owns or is otherwise responsible for them.

Again, these digital assets are rarely likely to entirely operate within a country's physical borders due to the advent or modern computing paradigms and global supply.

These global digital assets may be physical, virtual or logical across networks, hosts and services and potentially globally distributed. However, the existence, loss or compromise presents a potential national critical risk to the country.

As with the assets outlined in the previous section, we assert this class is challenging to both define or identify entirely. Thus precluding accurate assessment and quantification.

Summary and Conclusions

How countries define their digital borders and their digital assets is not we suggest universally understood, agreed or documented.

Achieving such definitions will become increasingly important in pursuit of international norms. national cyber resilience, global stability and agreement. This is due in part to multinationalisation, globalisation of supply chains and evolutions in computing & networking paradigms. Without such definitions governments risk not being able to articulate which are their assets nor accurately assess their levels of cyber risk stemming from their national attack surface due to vulnerability.

Taxonomy

The following table attempts to bring the described concepts into a taxonomy to aid further discussion and development.

Asset	National Digital Boundary	National Digital Asset	Sovereign	Physically in Country
Country Addressing	Yes	Yes	Yes	Yes
Country Assigned	Maybe	Yes	Yes	Maybe
Country Hosted	No	Yes	Yes	Yes
Country Controlled	No	Yes	Maybe	Maybe
Country Critical	No	Yes	Maybe	Maybe

Related Works

The discussion of digital borders and sovereignty has been ongoing for 20 years. Below are articles and papers related to this topic which may be interest to the reader.

POV: Why it's time for digital borders - May 2022 - General Robert Spalding and Michael Hochberg
https://www.fastcompany.com/90792643/pov-why-its-time-for-digital-borders

National Cyber Security Strategy and the Emergence of Strong Digital Borders - Winter 2020, Sanjay Goel
https://www.jstor.org/stable/26934537

Internet Sovereignty - October 2020 – Liam Hartley
https://medium.com/digital-diplomacy/internet-sovereignty-e2cb663337c2

Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? - 2018 – Forrest Hare
https://ccdcoe.org/uploads/2018/10/06_HARE_Borders-in-Cyberspace.pdf

Cyber Border Security – Defining and Defending a National Cyber Border - October 2017 - Phillip Osborn
https://www.hsaj.org/articles/14093

National boundaries have survived in the virtual world—and allowed national laws to exert control over the Internet - February 2006 - Jack Goldsmith and Timothy Wu
https://www.legalaffairs.org/issues/January-February-2006/feature_goldsmith_janfeb06.msp

Asserting National Sovereignty in Cyberspace: The Case for Internet Border Inspection – June 2003 - Oren Upton
https://www.researchgate.net/publication/235112846_Asserting_National_Sovereignty_in_Cyberspace_The_Case_for_Internet_Border_Inspection