Cybersecurity Policy Framework

A practical guide to the development of national cybersecurity policy

Author:
Kaja Ciglic, Microsoft

Contributors:
Angela McKay, Microsoft
John Hering, Wimmer Solutions
Theo Moore, APCO Worldwide

Contents

Introduction:
The need for a national cybersecurity policy framework

We live in a period of dramatic change powered by technology. The "Fourth Industrial Revolution" brings enormous economic and social opportunities for people, organizations, and governments. The substantial increase in internet connectivity, the explosion of the number of connected devices, and the rapid take-up of technologies such as cloud computing, advanced robotics, and artificial intelligence (AI) are fundamentally changing people's lives. They are also changing the way organizations do business and the way governments provide public services and engage with citizens.

At the same time, with every new system or device that is connected to the internet the scope for cyber-attacks grows, as do the consequences of successful attacks. As cyber-attackers become ever more sophisticated in their operations and cyber-criminals ever more ambitious, policy-makers have to respond.

The world is poised, therefore, on the threshold of a new era of possibility and risk due to these new technologies and their increasing ubiquity in our families, businesses and governments. As we embrace a generation of possibilities emerging from cloud and edge computing, we must also acknowledge that we have to take up fresh responsibilities. The price for a world where the only limits on individual and national opportunity are imagination and application of effort cannot be ignored. We must be vigilant, we must understand and foster trust, and we must put cybersecurity at the heart not just of technology but also policy.

The state has traditionally assumed responsibility for national security, citizen welfare, economic growth, public health and a range of aspects that are fundamental to the prosperity and well-being of a country. The internet has become such a pervasive part of public and private life that it is now a vital component in almost all of these areas of state responsibility. But what are the responsibilities of the modern state in providing cybersecurity for individuals, organizations and its own operations? How can governments think about using cybersecurity to help enable their country to benefit from the full potential of the internet?

Today's cybersecurity decisions shape tomorrow's success

The value of good cybersecurity law is not abstract. Research on a number of potential configurations of cyberspace in 2025 shows that policy decisions, notably in areas broadly defined as 'cybersecurity policy', can have significant 'real world' effects.

For developed economies the variance in R&D growth between best-case and worst-case scenarios could be as much as 18%, whilst for emerging economies it could be a difference of over 30%. Debt as a percentage of GDP could also be materially affected by the public and private sectors' ability to absorb and capitalize on new technologies.

Furthermore, in a hyper-connected, device-rich world (which describes 'emerging' and 'developing' states just as much as 'developed' ones), Internet stability and security will be critical. Equally important will be the structures and systems that enable effective cyber-risk management, as well as resilience and recovery in the face of cyber-attacks.

The cybersecurity policy framework that states adopt will, therefore, have a critical bearing on their prospects for growth, governance, and good practice.

In their responses policy-makers are compelled to balance competing priorities, e.g. the need for measures to tackle cyber-threats with the requirement to protect fundamental principles like privacy and civil liberties. In the same way, they must balance the need for regulations to enhance cybersecurity with the risk that those regulations, if not structured correctly, could stifle the innovation and progress being driven by technology.

Unlike many other bodies of national and international law, cybersecurity legislation has not had a chance to evolve over many decades, supported by established norms and consistent standards across many developed jurisdictions. For example, whereas privacy laws in many countries are now captured in a single, comprehensive statute, supported by a specific agency empowered to enforce the laws and raise national standards, cybersecurity regulations are often heavily-fragmented and, in some cases, key principles are yet to be addressed at all. Indeed, as cybersecurity is a relatively new and potentially very broad subject, it is being applied to everything from cybercrime to encryption, from critical infrastructure protection to content regulation.

Through the combined efforts of international organizations and leading governments, best practices in cybersecurity policies have started to emerge. There is still, however, no single point of reference for policy-makers tackling the issue of cybersecurity. Instead, faced with an incredibly complex subject, they are forced to dedicate substantial time and resources to building new frameworks almost from scratch, all the while leaving themselves, their citizens and local businesses exposed to the growing range of threats.

It is against this backdrop that Microsoft has developed this Cybersecurity Policy Framework. As a global technology company, Microsoft has been at the heart of discussions about cybersecurity between industry and governments around the world for many years. We have observed and been involved in the development of best practices in cybersecurity regulation, from outcomes-focused approaches to cybercrime laws to implementation of security baselines for critical infrastructures.

Designed as a practical guide for policy-makers, this Framework is part of a series of materials published by Microsoft to map out best practices and to arm policy-makers with what they need to develop comprehensive and robust cybersecurity regulations, particularly in areas such as appointing a national cybersecurity agency and drafting cybercrime and critical infrastructure protection regulation.

We believe that now is a critical moment for policy-makers. They must aim to craft a regulatory framework for cybersecurity that is fit for the changing landscape of the Fourth Industrial Revolution. We hope that the Cybersecurity Policy Framework helps to support this objective and look forward to continuing our work with

industry and governments around the world to develop an appropriate regulatory framework for cybersecurity.

How to use the Cybersecurity Policy Framework

The Cybersecurity Policy Framework is designed for policy-makers involved in the development of cybersecurity regulations. It is not intended to exhaustively address all of the key parts of a country's national or international cybersecurity strategy but, rather, to provide a practical guide to the specific areas of cybersecurity regulation that policy-makers are currently most focused on.

The Cybersecurity Policy Framework is accompanied by a growing range of cybersecurity resources that Microsoft has published to support policy-makers. For access to these resources, see the "Recommended resources" section of this paper or visit the Microsoft cybersecurity policy website at microsoft.com/en-us/cybersecurity.

Chapter 1

Microsoft's commitment to cybersecurity

In today's complex and regulated environment, businesses need to focus on building more secure solutions that deliver value to their customers, partners, and shareholders—both in the cloud and on-premises. Microsoft has decades-long experience building enterprise software and running some of the largest online services in the world. We use this experience to implement and continuously improve security-aware software development, operational management, and threat-mitigation practices that are essential to the strong protection of services and data.

At any point in time on any day of the week, Microsoft's cloud computing operations are under attack: The company detects a substantial number of attempts a day to compromise its systems. Microsoft has an unrivaled vantage point on digital security because our products are in use by billions of people around the world, which means we often serve as the first line of defense against bad actors seeking to cause harm to personal information and business networks.

However, Microsoft isn't just fending off those attacks. It's also learning from them. All those foiled attacks, along with data about the hundreds of pieces of raw data that we see such as anonymous, signature-free signals from our products, 450 billion authentications per month across all our cloud services, 400 billion emails analyzed for malware and malicious sites, – can be combined to help us, for example, to connect the dots between an email phishing scam out of Nigeria and a denial-of-service attack out of Eastern Europe. That means we can thwart one attack for one customer and then apply that knowledge to every other customer using our products, from our Azure computing platform, to Windows 10 operating system or the Office 365 productivity service. In other words, every incident becomes a learning opportunity that makes us stronger, faster and more agile in providing security and protecting trust.

Today, multiple layers of defense-in-depth, both in hardware and in software, are required to repel hackers. Microsoft has embraced it for some time and we pursue a cross company approach to cybersecurity. This means that beyond our focus on the secure development and secure operation of our products and services, we also invest substantially in the security of our company and create groups within the company that focus on protecting both ourselves and our customers:

- **The Cyber Defense Operations Center** is an state-of-the-art facility staffed 24/7 with experts from around the world who have been drawn from every division of Microsoft. These experts assess new threats from every vantage point and layer of complexity, and work directly with customers.

- **The Digital Crimes Unit** is where the company works directly with law enforcement organizations around the world to pursue legal recourse against cybercriminals by referring criminal cases to authorities or bringing civil cases ourselves.
- Moreover, **Microsoft's Global Cybersecurity Strategy and Diplomacy (GSSD) Team** partners with governments and policymakers around the world, blending technical acumen with legal and policy expertise. By identifying strategic issues, assessing the impacts of policies and regulations, leading by example, and driving groundbreaking research, they help to promote a more secure online environment.

However, Microsoft also realizes that security cannot be proprietary and that trust cannot be commoditized. Security is a fundamental right, and delivering it must be a mission we all share. Indeed, providing for the common defense has been a part of our global culture for generations. We know that the industry must come together to create as strong a shield as possible against the invisible threat if cyber-attackers and their cyber-weapons; as a result we have convened and enabled a number of alliances, such as the Cybersecurity Tech Accord, to protect citizens around the world.

Chapter 2

Introducing key concepts in cybersecurity policy

Introducing key concepts in cybersecurity policy

There are many terms associated with cybersecurity and these can be interpreted differently by stakeholders. However, having a common understanding of the terms and how they relate to one another is essential. In this section, we briefly introduce some of the key underlying terms. These definitions are not intended to be comprehensive, nor are they intended to form the basis of any legal or regulatory definition. Instead, they provide high-level assistance in understanding the key concepts as they are now widely understood, ahead of them being explored in more detail later in this Cybersecurity Policy Framework.

Cybersecurity

The protection of connected systems and networks, and the data stored on those systems and transferred via those networks, from attack, damage or unauthorized access.

Cybersecurity norms

Agreed expectations for the behavior of state actors in cyberspace at an international level - e.g., the need for states to cooperate in preventing international cybercrime.

Critical Infrastructure (CI)

Systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Information security

Protecting information from unauthorized access, use, disclosure, disruption, modification or destruction.

Security Baselines

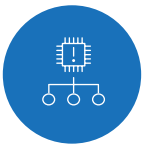
The minimum security standards required for information security systems.

Information assurance

The steps involved in ensuring information security.

International standards

Typically refers to international security standards, such as ISO/IEC standards, against which organizations can measure their security practices.



Critical information infrastructure (CII)

Information and communication systems forming part of CI (see above) whose maintenance, reliability and safety are essential for the proper functioning of the CI and/or the country as a whole.

Security controls

Specified measures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

Chapter 3

Overview of the Cybersecurity Policy Framework

This Cybersecurity Policy Framework focuses on three key regulatory aspects of cybersecurity policy, framed by a wider national strategy as well as an international strategy for cybersecurity.

A national strategy for cybersecurity

A national strategy for cybersecurity

What is a national strategy for cybersecurity?

A national cybersecurity strategy outlines a country's cybersecurity vision and sets out the priorities, principles, and approaches to understanding and managing cybersecurity risks at a national level.

Why is a national strategy for cybersecurity needed?

Any regulatory framework for cybersecurity needs be based upon a principled national strategy. The national strategy should set clear, top-down direction to establish and improve cybersecurity for government, organizations, and citizens. Such a strategy is essential for managing national-level cybersecurity risks and for developing appropriate regulation to support those efforts.

What makes a successful national strategy for cybersecurity?

Priorities for national cybersecurity strategies will vary by country. In some countries, the focus may be on protecting critical infrastructure. Other countries may focus more on protecting intellectual property. And others may focus more on improving the cybersecurity awareness of citizens. In most cases, the strategy will incorporate a combination of these items.

In Microsoft's experience, the most successful national strategies share three important characteristics.

- First, they are embedded in **"living" documents** that have been developed and implemented in partnership with key public and private stakeholders. They are sufficiently flexible to adapt to the changing cybersecurity landscape.
- Second, they are based on **clearly articulated**

National cybersecurity plans can accelerate growth and development

ICT development accelerates business and economic growth, as technological sophistication is a multiplier for economic and social development, which in turn drives further technological development.

A national approach to cybersecurity is essential to that acceleration, if it is flexible, proportionate and outcomes focused. Government must strive to keep up with a rapidly evolving technology environment, regularly clarify its role in "cyber", review its policies and update its own systems.

The temptation to use cybersecurity policy for well-intended purposes, i.e. to protect/favor/stimulate a domestic sector or to exclude foreign companies that are a national security concern, is likely to be counter-productive if it suppresses the vitality brought by competition and global ICT access.

principles that reflect societal values, traditions, and legal principles. Programs created by government in the name of security can potentially infringe on these rights and values if not articulated and integrated as guiding principles.

- Third, the strategies are based on a **risk-management approach** where governments and private sector partners agree on the risks that must be managed or mitigated, and even those that must be accepted.

Key policy principles

The national cybersecurity strategy should set out the key principles that will guide the preparation and enforcement of cybersecurity policies. Microsoft recommends the following six foundational principles as the basis for cybersecurity policy:

1. **Risk-based and proportionate**. Regulations should be based on a thorough understanding of the threats, vulnerabilities, and potential consequences facing the country. Policy-makers should develop frameworks and systems that are proportionate and specifically designed to address these threats, vulnerabilities and potential consequences. As part of this, policy-makers need to consider the fact that the definition of "risk" itself is changing. In the past, "risk" may have meant doing something new or adopting a disruptive new technology. Today, "risk" can mean standing still, because organizations and even countries that stand still will lose competitiveness and be overtaken. Regulations can manage this by introducing a proportionate, risk-based framework that enables organizations to innovate and adopt new technologies without exposing the country to unnecessary cybersecurity risks.
2. **Outcome-focused.** It is essential that regulations focus on delivering the desired end state, rather than prescribing the means to achieve it, and then measure progress towards that end state. In the rapidly-changing world of cybersecurity, prescriptive approaches will quickly become out-of-date or leave the country out-of-step with international best practices.
3. **Prioritized.** Not all threats are equal. Cybersecurity policy should adopt a graduated approach to criticality, prioritizing critical infrastructure risks.
4. **Practicable and realistic.** Cybersecurity policies are of little value if they impose undue burdens on the organizations who must comply with them or on the authorities tasked with enforcing compliance. Engagement with industry and the relevant authorities is a necessary first step to ensuring that policies are practicable and realistic.
5. **Respectful of privacy, civil liberties, and rule of law.** Enforcing cyberspace

cannot come at a cost of sacrificing privacy, civil liberties, and rule of law. For example, broad rights for government and law enforcement to access data without following appropriate processes (such as obtaining necessary warrants) can cut across these fundamental principles. This in turn can damage the country's reputation for rule of law and ultimately disincentivize organizations from storing their data within the country. Instead, a balanced approach is needed that is respectful of these fundamental principles.

6. **Globally-relevant.** The threats to cyberspace do not stop at national borders. It is therefore essential that governments adopt approaches for tackling cybercrime and encouraging cybersecurity that acknowledge that reality. National approaches should therefore integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible.

Further information

To assist policy-makers in the development of a national cybersecurity strategy, Microsoft has published a guide, based on its experience of emerging best practices around the world. The guide, "Developing a National Cybersecurity Strategy", is available at microsoft.com/en-us/cybersecurity/.

Establishing and empowering a national cybersecurity agency

Establishing and empowering a national cybersecurity agency

What is a national cybersecurity agency?

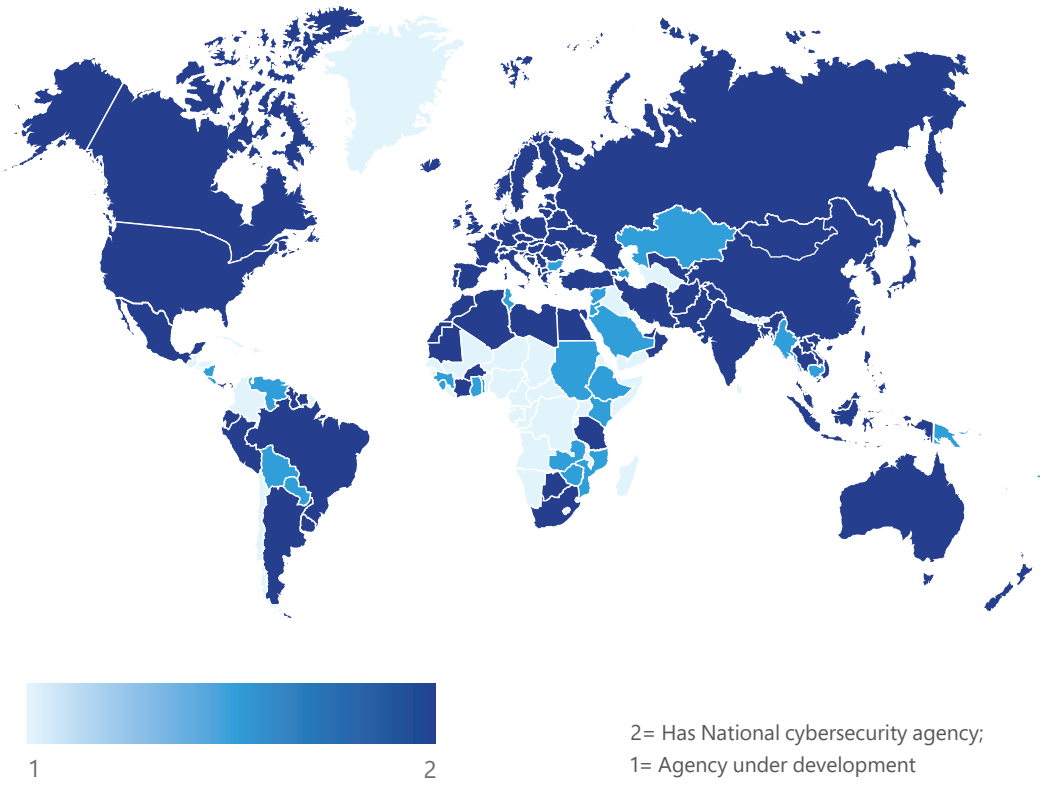
Many countries around the world have established, or are looking to establish, civilian agencies or other administrative bodies to manage the country's cybersecurity strategy. Countries as diverse as Australia, France, Israel, Japan and Singapore, to name just a few, already have specific bodies of government responsible for cybersecurity. The move towards establishing national cybersecurity agencies[1] reflects the increased inter-dependencies caused by the digital transformation, as well as the perceived and real growth of cyber-threats.

Why is a national cybersecurity agency needed?

Because cybersecurity touches all aspects of our society, establishing a well-functioning agency will benefit the broader cybersecurity ecosystem. These type of agencies have unique authorities that allow them to address cybersecurity directly, but also perform an essential function in coordinating across different organizations in the country - government and private. As governments around the world begin to consider creating or restructuring their own national cybersecurity agencies, this Cybersecurity Policy Framework offers a set of best practices to guide their development. The proposed structure stems from Microsoft's internal frameworks for responding to cyber incidents and driving partnerships with government and industry, and is also based on examples of

[1] The legal and administrative structure of the bodies of government responsible for cybersecurity will inevitably differ from one country to the next. Nonetheless, for convenience, we refer to these bodies in general terms as "national cybersecurity agencies".

MAP: Countries with established or developing a national cybersecurity agencies[13]



cybersecurity agencies around the world.

Allowing for many different forms that a national cybersecurity agency can take, our experiences of working with governments around the world indicate that there are some particularly effective approaches to structuring them. These include approaches to how they are structured operationally, how their roles are viewed, and which responsibilities they are assigned. The five recommendations for structuring an effective national cybersecurity agency are:

1. **Appoint a single national cybersecurity agency:** Having a single cybersecurity agency at a national level (as opposed to a fragmented approach, which may include various cybersecurity teams spread across different agencies) is essential to creating and implementing a coordinated national cybersecurity policy, both for government infrastructure and for the broader ecosystem. While cybersecurity concerns are likely to cut across many "traditional" government agency policy areas, such as justice, treasury, defense, or foreign affairs, having a centralized authority will help establish a horizontal

baseline of cybersecurity best practices which the different sector-specific verticals can build off.

2. **Provide the national cybersecurity agency with a clear mandate:** Any national cybersecurity agency will be expected to navigate a complex environment that spans other government departments, national legislatures, established regulatory authorities, civil society groups, the general public, public and private sector organizations, and international partners. It is therefore important that all stakeholders have a clear expectation of what the mandate of the national cybersecurity agency is, so they know what to expect and who to talk to. It is also critical that the responsibilities of the national cybersecurity agency are distinct from those of other governmental groups touching on cybersecurity. One such example are regulators in critical infrastructure sectors, such as financial services, power generation or transport, which can set security policies for their industry in some contexts.

3. **Ensure the national cybersecurity agency has appropriate statutory powers:** Currently, most national cybersecurity agencies are established not by statute but by the delegation of existing powers by other parts of government. We anticipate that this approach will need to change in some countries as they pass comprehensive cybersecurity laws. In the same way as the passage of comprehensive data protection laws led to the establishment of specific bodies to enforce the relevant laws, e.g. the Australian Information Commissioner Act, so too is this likely to be required for the enforcement of comprehensive cybersecurity laws. The delegation of existing powers, which may be subject to multiple underlying regulations, may not be sufficient to provide the National Cybersecurity Agency with all of the powers it requires to effectively carry out its new functions.

4. **Implement a five-part organizational structure:** The ideal competent authority would resemble a cybersecurity agency composed of five parts. This five-part structure allows for a multifaceted interaction across internal

Many possible types of agency but all with one essential purpose

A national cybersecurity agency, if appropriately structured, can substantially increase the readiness of a country's cybersecurity ecosystem, with many of the economic and developmental benefits already outlined.

The creation of such an agency can follow many paths, e.g. by delegation of existing powers from other parts of government to a standalone body or by creation of multiple agencies with clear briefs focused on distinct aspects of cybersecurity.

In all cases, however, public-private partnership and cooperation will be key because much of "cyberspace" is built, owned and operated by the private sector. Obstructive dynamics between a national cybersecurity agency and businesses, not to mention with peer agencies in other states, will be counterproductive.

government and regulatory stakeholders and external stakeholders from the public and private sectors, as well as the international arena. In particular it addresses one of the core challenges governments have faced in establishing national cybersecurity agencies: how to reconcile mandatory reporting of cyber-incidents, as handled by the Regulatory unit, with the voluntary and bi-directional exchange of information about cyber-threats and -incidents, as handled by the CERT:

a) **Policy and planning unit:** This unit should lead the nation's development, coordination, alignment, and integration of cybersecurity policies, strategies and plans. It should define near-, mid-, and long-term strategic priorities, develop plans to implement those priorities, and it should track and monitor progress against the plans.

b) **Outreach and partnership unit:** This unit should lead and manage relationships and interfaces across the government and with other nations, institutions, and the private sector. The Outreach and partnership unit should create and manage intra- and inter-governmental advisory councils and public private partnerships (PPP) to enable collaboration.

c) **Communications unit:** The Communication unit should coordinate regulatory and non-regulatory communication, including messages, documents and publications, and statements to all stakeholders on behalf of the national cybersecurity agency. The Communication unit should serve as the lead for communication during a crisis or emergency, and the primary point of contact for media, organizations and the general public seeking information about the agency's programs, policies, procedures, statistics, and services.

d) **Operations unit:** The operations team should be tasked with ensuring effective coordination and deployment in response to cyber threats. As such, the operations team should consist of a communications unit as well as a CERT.

e) **Regulatory unit:** This unit should be responsible for overseeing compliance with cybersecurity regulations. This would include developing guidance to help organizations understand the relevant requirements, interacting with regulators who will enforce compliance, establishing an incident reporting framework, and collaborating with other units to update regulatory obligations.

Further information

To learn more about the existing cybersecurity agency models, see:

- Australian Cyber Security Centre (ACSC): acsc.gov.au/
- National Cybersecurity Agency of France (ANSSI): ssi.gouv.fr/en/
- The National Cyber Bureau of Israel: pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx
- Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC): nisc.go.jp/eng/
- Singapore Cyber Security Agency (CSA): csa.gov.sg/

Developing and updating cybercrime laws

Developing and updating cybercrime laws

What are cybercrime laws?

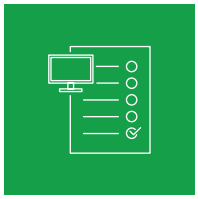
A country's approach to cybercrime laws will largely be dependent on the country's existing laws, legal structures and traditions. While some countries have elected to introduce stand-alone cybercrime laws, others have incorporated them into legal frameworks that deal with the overall online environment, such as broader electronic commerce laws. In Microsoft's experience, however, all effective frameworks incorporate the following six objectives:

1. Deterring perpetrators and protecting citizens

2. Enabling law enforcement investigations while protecting individual privacy

3. Enabling cooperation between countries in criminal mattersinvolving cybercrime and electronic evidence

4.



Setting clear standards of behavior for the use of computer devices

5.

Requiring minimum protection standards in areas such as data handling and retention

6.

Providing fair and effective criminal justice procedure

Why are modern legal frameworks to fighting cybercrime needed?

Governments are struggling to respond to the growing threat, sophistication and prevalence of cybercrime, as both the pace of technological development and frequency of activity by cybercriminals and other malicious actors, far outstrips the development of legal frameworks. Microsoft therefore believes that governments must adopt new approaches and put forward legal frameworks that are flexible enough to allow rapid responses to new challenges and are designed so that they do not become obsolete. Furthermore, we believe that the global challenge of cybercrime will only be addressed through harmonization of cybercrime laws, combined with initiatives to facilitate faster and more effective coordination between law enforcement agencies.

Cybercrime laws benefit the economy

Cybercrime laws are one of the foundations that are needed to protect the society from online attacks. They perform an important deterrent role, helping reduce the level of crime in a given country.

Given the global nature of cybercrime activity they are not only essential for ensuring that a particular country does not become a safe haven for criminals, but they also enable prosecutors to cooperate with other countries in bringing those criminals to justice.

Cybercrime laws also play a critical role in attracting foreign investment. With much of intellectual property online today, companies want to know that they will be able to protect their investment should it come under attack.

What makes a successful cybercrime policy?

An effective legal framework for cybercrime should be based on six broadly-applicable best practices:

1. **Establish the necessary investigative powers:** To effectively investigate the growing range of cyber-threats, authorities will need new, clearly-defined investigative powers. For example, to secure non-physical, intangible evidence generated by cybercrime, investigators will need to be able to access, often remotely, various types of stored data. In developing these powers, it is essential that there is a clear scope of application of the power to guarantee legal certainty in respect of its use; and that sufficient legal authority, e.g. obtaining a search and seizure warrant when seeking access to content, is required in order to exercise the relevant powers.
2. **Enable and facilitate cooperation with the private sector:** Governments and law enforcement cannot win the battle against cybercrime on their own. Working with industry on best practices and emerging issues allows governments to take advantage of the expertise and resources of the private sector in the fight against cybercrime. To ensure that can happen, cybercrime laws should: i) create safe harbors to enable rather than

inadvertently criminalize researchers and appropriately-regulated private investigators; ii) enable information and data sharing between the public and private sectors, and within the private sector; and, iii) permit limited and appropriately-regulated private enforcement and/or active defense, provided that appropriate controls are in place to ensure that this does not extend to 'vigilante' or 'hack back' behaviors.

3. **Balance those investigative powers with baseline principles such as privacy and civil liberties:** While establishing appropriate investigative powers is a necessary step in tackling cybercrime, policy-makers must balance this with existing privacy expectations, laws and norms. Failing to find the right balance can, in more extreme cases, make the investigation or enforcement worse than the crime. To find the right balance, Microsoft believes that: i) access to traffic data should be subject to a "due cause" test; access to any other type of data (e.g. content) should require a court order; and the relationship between investigative powers and privacy is specifically called-out in the relevant cybercrime regulation.

4. **Define crimes in an outcome-focused way:** The definition of "crime" is changing. In an increasingly complex online environment, it is challenging to assess who is the victim, who is the perpetrator, and even whether a crime has been committed at all. Microsoft encourages policy-makers to complement existing definitions of criminal acts with new thinking about what constitutes a criminal outcome. In defining cybercrimes, it is essential that the definitions are specific enough to be workable whilst broad enough and forward-looking enough to encompass new, as yet unknown tactics that cyber-criminals may employ. This approach ensures that as technology continues to develop, outcome-focused laws can still apply.

An International Benchmark for Cybercrime Laws – the Budapest Convention

The Convention on Cybercrime of the Council of Europe, commonly referred to as the Budapest Convention, is the preeminent binding international instrument in the area of cybercrime. It serves as a guideline for countries developing national legislation and provides a framework for international cooperation between countries' law enforcement agencies, so critical to cybercrime investigation and prosecution. Its influence extends far beyond the countries that have singed it, with a number of international organizations participating in the Convention Committee and many other countries looking at it for best practices.

For more information, see:

- The Budapest Convention: https://www.coe.int/en/web/cybercrime/the-budapest-convention

5. **Rely on accepted definitions:** As cybercrime often crosses borders, it is important that the law enforcement agencies involved in investigating it have a broadly similar understanding of what crime has taken place. The solution to this challenge lies in the adoption of cybercrime laws that are consistent with broadly-accepted international standards. For example, the Council of Europe's Budapest Convention provides a good model for cybercrime legislation that harmonizes laws and facilitates cooperation across borders.
6. **Build global cooperation:** Cybercrimes, like the internet, are borderless. Effective enforcement therefore depends on cooperation between governments, law enforcement and organizations across multiple jurisdictions. While there has been some progress on an international scale, the matrix of overlapping regional approaches and standards in how to address cybercrime continues to cause problems for law enforcement and therefore opportunities for cybercriminals. A concerted effort is needed towards greater global harmonization in three core areas: i) tackling criminal safe havens; ii) addressing the principle of dual criminality; and, iii) Enabling global evidence collection.

Further information

For more information:

- Microsoft Digital Crimes Unit Newsroom: microsoft.com/presskits/dcu/
- Microsoft paper, "Modern Cybercrime Policy": query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVtZW

Developing and updating critical infrastructure protection laws

Developing and updating critical infrastructure protection laws

What is critical infrastructure?

Modern life is increasingly reliant on a wide-ranging set of functions, services, systems, and assets, commonly referred to as infrastructures. Today, governments view several of these infrastructures, such as communications, banking, energy, transportation, and healthcare, as critical, since their disruption, destruction, or loss of integrity can impact a nation's stability. Critical infrastructures are often thought of as physical assets.

Critical Infrastructure: A Definition

While the appropriate definition of "critical infrastructure" may differ somewhat from one country to the next, Microsoft believes the following definition, based on that implemented by the National Institute of Standards and Technology (NIST) in the United States, strikes the right balance of specificity and future-proofing:

"'Critical Infrastructure' means systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Why are legal frameworks needed to protect critical infrastructure?

ICT is increasingly central to the social and economic opportunity of the world today. This is also true of critical infrastructures. These entities are embracing digital connectivity and leveraging it to drive down cost, increase productivity and efficiency, improve service delivery, and ultimately to enable greater economic opportunity. However, the connection of critical infrastructures via networks brings new risks.

The essential nature of the critical infrastructures' function and services renders their protection an important national policy concern. However, unlike traditional, offline, security approaches, which could often be mitigated through regulatory action alone, understanding and managing risk to infrastructures connected to

digital environments requires a new approach. The complexities involved can only be navigated through unprecedented coordination and collaboration across government, critical infrastructure owners and operators, as well as technology vendors.

What makes for effective critical infrastructure protection policy?

While many countries already have developed critical infrastructure protection laws, those laws are often heavily fragmented, usually spread across several sector-specific regulations and operator license conditions. In many cases, the requirements predate the widespread adoption of new technologies in critical infrastructure or are struggling to keep pace with technological developments. For these reasons, there is now an urgent need for measures aimed at the prevention, handling of, and the response to risk and incidents affecting critical infrastructures. The following constitute best practices that Microsoft has found effective:

1. **Identify critical infrastructures:** One of the most important aspects of critical infrastructure protection is identifying which infrastructures are critical, in collaboration with owners and operators and other appropriate representatives of the private sector and government. A detailed risk assessment should guide the identification and prioritization of critical infrastructures. The list of critical infrastructures should be sufficiently specific as to be workable and not unduly broad to ensure that resources are prioritized and focused on those assets that need to be protected most. The national cybersecurity agency should periodically review and update the applicable criteria and identified critical infrastructure.
2. **Understand the scope and status of existing policies and capabilities:** To establish a national-level critical infrastructure protection program or review an existing one, it is important to first understand the scope and status of existing policies and security programs, as well as identify existing operational capabilities. A policy review will help determine what policies, authorities, organizations, and capabilities are currently in place, and what gaps, if any, exist.
3. **Empower a central authority to implement critical infrastructure protection policies:** To overcome the potentially fractured nature of the policy and risk environment, the government should appoint a single authority, e.g. the national cybersecurity agency, to oversee the implementation of critical infrastructure protection policies. Its role should include: i) conducting sector-

specific risk assessments and identifying categories of critical infrastructure; ii) coordinating the adoption of outcome-based cybersecurity practices; iii) establishing an incentives-based cybersecurity program to encourage outcome-based practices; iv) developing procedures to inform owners and operators of cyber-threats, vulnerabilities and consequences; and v) providing technical guidance and support.

4. **Clarify the respective responsibilities of owners and operators of critical infrastructure:** There should be a clear distinction between an "owner" and an "operator" of critical infrastructure. Owners of critical infrastructure may own the infrastructure but they are not always able or best placed to comply with the statutory obligations because they usually do not operate the computer systems that process the data on a day-to-day basis. Operators, meanwhile, are the entities that manage or operate the critical infrastructure. The relevant obligations may include: implementation of regular system audits by approved third-party auditors or performing regular risk assessments on critical infrastructure.

5. **Introduce minimum security baselines for critical infrastructure:** The national cybersecurity agency should establish minimum security baselines for critical infrastructure. These can take form of voluntary guidance, coupled with incentives, e.g. procurement requirements or tax subsidies; or be implemented through a mandatory regulatory requirement, in particular where an elevated need for assurance arises from the risk environment. The measures that apply should be proportionate to the criticality of the infrastructure, based on international good practice standards, such as those set out under the NIST Cybersecurity Framework. It is important that these security standards are developed in close collaboration with the industry to ensure that they are realistic and practicable.

Adjusting risk management and catalyzing economic growth

Globally aligned security baselines ensure that sufficient resources are applied to security and risk management rather than diverted toward compliance. Throughout the ecosystem, the impact of this is multiplied, as third party suppliers are also able to devote sufficient resources to security and risk management rather than diverting those resources toward compliance.

Moreover, they can ensure that organizations continue to invest in security innovation, as organizations have confidence that policies provide sufficient flexibility to develop new techniques, capabilities, and architectures.

Finally, security baselines can help ensure that organizations continue to invest in and leverage resources across borders, maintaining the global manufacturing and outsourcing relationships that have helped to not only increase global economic opportunity but also drive down the costs of developing and popularizing advanced technologies.

6. **Encourage information sharing:** Sharing threat-based information such as vulnerabilities, hacking trend data, new threat identification, or even unexplained anomalies impacting a product or service can enable the IT sector and government to better protect critical systems and respond to emerging issues. Not only is it the case that when information about attackers and methods of attack is shared, organizations are better prepared to thwart them, it can also help lead to new protections or mitigations, sometimes even before any impact. Microsoft believes that a sustainable information sharing program needs to be event-driven and to focus on several key areas that should be precisely defined: the actors involved, the type of information exchanged, whether sharing is voluntary or required, the methods and mechanisms for transmitting information, and the grouping of actors in a program.

Security Baselines best practice: NIST Cybersecurity Framework

The Framework for Improving Critical Infrastructure Cybersecurity, developed by the United States National Institute of Standards and Technology (NIST), is an example of a security baseline that has proven to be effective and has therefore quickly gained broad adoption, also outside the United States. Its usefulness can, at least in part, be attributed to the nature of its development process. The Framework was developed in close collaboration with the industry – across different sectors and sizes – in an iterative, consultative process.

The NIST Framework began life as Executive Order 13636 on Improving Critical Infrastructure Cybersecurity. Its development took place over many months through official consultations, workshops, and informal conversations. The Framework continues to evolve and be updated, as through implementation stakeholders discover challenges or areas to which it could expand to help them manage their cybersecurity risk environment.

Critically, the United States is not the only geography looking to utilize the Framework. In Europe, the Italian government in 2015 adopted their own cybersecurity framework, which focuses on small and medium sized enterprises. The Italian document is largely grounded in the NIST Framework. Similarly, the Australian Securities and Investments Commission (ASIC) in 2015 issued Report 429 Cyber resilience: Health check (REP 429), which encouraged businesses to consider using the NIST Cybersecurity Framework to assess and mitigate their cyber risks or to stocktake their cyber risk management practices.

The uptake of the Cybersecurity Framework is likely to continue. The recent Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure mandates the use of the Framework across the agencies of the United States government. Moreover, the International Standards Organization (ISO) has recently approved work on a technical report on "Cybersecurity and ISO and IEC Standards", which seeks to take the NIST Cybersecurity Framework and adapt it to the international environment.

7. **Create public private partnerships:** Public-private partnerships are a cornerstone of effectively protecting critical infrastructure and managing security risks in both the short- and long-term. They are essential for boosting trust amongst and between the operators and the government. Their focus areas could include: coming to an agreement on common cybersecurity baselines, establishing effective coordinating structures and information-sharing processes and protocols, identifying and exchanging ideas, approaches, and best practices for improving security, as well as improving international coordination.

Further information

For more information, see:

- "Critical Infrastructure Protection: Concepts and Continuum": query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVtZU
- "Cybersecurity Policy Toolkit: Mandatory Incident Disclosure Models": https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW5Alw
- "Risk Management for cybersecurity: Security Baselines"
- http://download.microsoft.com/download/4/6/0/46041159-48FB-464A-B92A-80A2E30B78F3/MS-riskmanagement-securitybaselines-WEB.pdf

An international strategy for cybersecurity

An international strategy for cybersecurity

Why is an international strategy for cybersecurity needed?

Cybersecurity is a challenge that transcends territorial boundaries. At the same time, governments continue to invest in greater offensive capabilities in cyberspace, and nation-state attacks on civilians are on the rise. It is therefore more important than ever that states work together to address the growing range of cybersecurity threats. Any national strategy for cybersecurity must therefore have the international in mind too.

A country's national policies must enable the country to collaborate effectively with international partners and to design and comply with international obligations. To be truly effective, international norms for cyberspace will need to be implemented at a national level. Policy-makers must therefore keep the goal of international norms in mind when developing their national-level cybersecurity strategy and associated policies.

The risks of cyber-conflict demand effective support for international norms of behavior in cyberspace

Conflict in the real world is generally harmful to the economic and social structures and performance of those states directly involved. If the conflict is severe enough it can even negatively affect uninvolved states, for example by disrupting regional or global trade.

Conflict in cyberspace can be equally detrimental to states' growth and development. That being said, with the internet facilitating anonymity, it can be hard to attribute responsibility for state-supported cyberattacks during "peace time".

Contributing to international norms processes that reduce the risks of such attacks, let alone all-out conflict, should therefore be seen as a positive step for any country's future prosperity and stability. Indeed, for external investors and businesses, a market's clear commitment to minimize the risks of cyberconflict with neighbors and global partners will be regarded as a net positive.

What are cybersecurity norms and why are they important?

Norms are shared expectations of what behaviors are appropriate and inappropriate among members of a society. Common societal expectations about use of seat belts in cars and when or where to cross streets are norms from the physical world. In the context of international security, norms are intended to increase predictability and confidence between states in times of uncertainty. Norms are intended to deter actions by defining what behaviors are acceptable and unacceptable, and imposing consequences when states actions don't adhere to the defined behaviors.

To be clear, norms are not hard law. Norms are most often voluntary and/or politically binding agreements, and are an initial step in a cadence of

progress that can eventually evolve into customary international law and also pave the way for codification.

Microsoft believes that cybersecurity norms are essential if countries are to increase the security of cyberspace and to preserve the utility of a globally connected society. They should define acceptable and unacceptable state behaviors, with the aim of reducing risks, fostering greater predictability, and limiting the potential for the most problematic impacts.

What is the "Digital Geneva Convention"?

Beyond international cybersecurity norms, Microsoft believes that a Digital Geneva Convention is needed. The Digital Geneva Convention would commit governments to adopt and implement norms that have been developed to protect civilians on the internet, without introducing restrictions on online content. Just as the world's governments came together in 1949 to adopt the Fourth Geneva Convention to protect civilians in times of war, a Digital Geneva Convention would protect citizens online in times of peace.

We believe that to make significant progress in this space, we have to lay bare the fact that there is, unfortunately, little specificity in the government agreements reached so far. This situation allows states to continue to act in violation of established norms, without the international community having any recourse to respond. For example, international law prohibits the use of force by states except in self-defense in response to an armed attack, and the UNGGE norms call for states to refrain from international malicious activity. The questions are how these statements should apply to cyberspace, how concepts such as malicious activity are defined. This is where the work so far falls short. To move forward, these gaps will need to be identified and addressed.

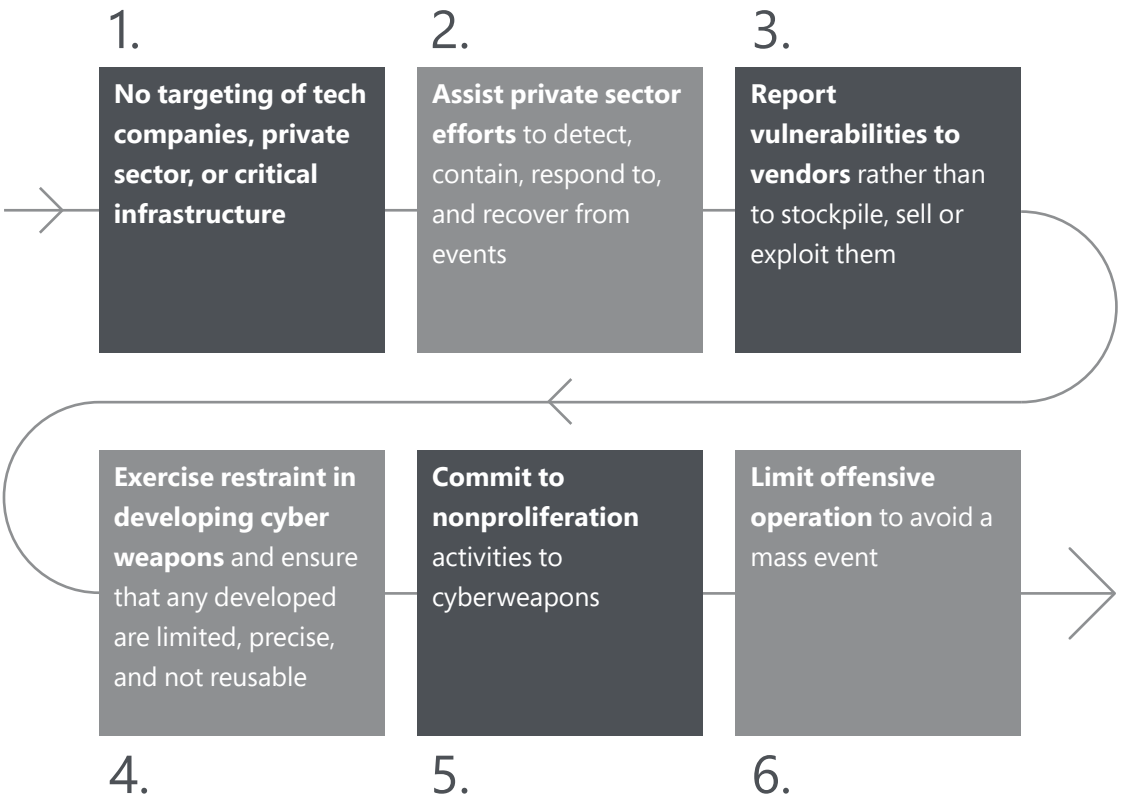
Moreover, the current list of norms does not fully address the core drivers of instability in cyberspace. A limited set of additional cybersecurity norms in areas where existing rules are either unclear or may fall short in protecting civilians in cyberspace need to be developed. This could include norms which explicitly articulate protections for civilians, even if they are implicitly contained elsewhere in international law. The development of these norms should be informed not just by governments, but also by civil society and the private sector.

While there is a need for urgency and even high ambition, steps can also be taken incrementally. There are important opportunities to progress towards a legally binding agreement through initial voluntary or politically binding efforts, such as those underway within the United Nations or the Group of Twenty Countries

(G20). Ultimately, whatever the route, arriving at a legally binding framework would establish new rules for governments and help protect cyberspace in both peacetime and prevent conflict

Which international cybersecurity norms should be adopted first?

A Digital Geneva Convention



Microsoft's proposal for a Digital Geneva Convention: Overview

Further information

Microsoft has long advocated for international norms to govern government behavior in cyberspace. To this end a series of white papers have been developed, putting forward suggestion for what form international cybersecurity norms could take. The white papers also examine the respective roles of public and private organizations. For more information, see:

- International Cybersecurity Norms - Reducing Conflict in an Internet Dependent World: microsoft.com/en-us/download/confirmation.aspx?id=45031
- The Need for a Digital Geneva Convention: blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

Overview of the Cybersecurity Policy Framework

Conclusion

At this time of unprecedented technological change, it is more important than ever that policy-makers rise to the challenge of developing cybersecurity policies that balance the new risk environment with the almost unlimited potential of technology to enhance the national and global good.

Decisions made by policy-makers over the next few years concerning matters such as cybercrime, protection of critical infrastructure, law enforcement and international cooperation will shape trust in computing and economic growth for decades to come.

To succeed in this new environment, it is essential that governments, citizens, businesses and organizations work together to create an appropriate cybersecurity policy framework, one that protects fundamental principles like privacy and civil liberties, encourages innovation and progress, and effectively tackles the growing range of cyber-threats.

We hope that this Cybersecurity Policy Framework is a useful starting point for policy-makers as they look to find solutions to the problems of this challenging new environment. We look forward to continuing both our collaboration with policy-makers around the world and our support for global efforts to make the future of computing more secure.

Recommended resources

Microsoft cybersecurity policy: www.microsoft.com/en-us/cybersecurity

A Cloud for Global Good: news.microsoft.com/cloudforgood/

Microsoft Trust Center: microsoft.com/en-us/trustcenter/


Microsoft