Inter-American Development Bank

Advanced Experiences in Cybersecurity Policies and Practices

An Overview of Estonia, Israel, South Korea, and the United States

Author:
James Andrew Lewis

Editors:
Miguel Angel Porrúa
Ana Catalina García de Alba Díaz

Institutions for Development Sector

Institutional Capacity of the State Division

DISCUSSION PAPER Nº IDB-DP-457

July 2016

Advanced Experiences in Cybersecurity Policies and Practices

An Overview of Estonia, Israel, South Korea, and the United States

Author:
James Andrew Lewis

Editors:
Miguel Angel Porrúa
Ana Catalina García de Alba Díaz

July 2016

IDB
Inter-American Development Bank

Contact: Miguel Angel Porrúa, mporrua@iadb.org.

OBSERVATORY
CYBERSECURITY
IN LATIN AMERICA AND THE CARIBBEAN

Advanced Experiences in Cybersecurity Policies and Practices

An Overview of Estonia, Israel, South Korea, and the United States

IDB
Improving lives

Abstract

Access to the Internet increases productivity, national income, and employment. Access to information catalyzes growth. However, these opportunities come with risk. Digital technologies are not mature and can be easily exploited by criminals and other antagonists. This discussion paper looks at the experience of four countries—Estonia, Israel, South Korea, and the United States—that are among the most advanced in cybersecurity, to see how they have tackled this problem and what lessons can be learned from their experiences. To provide a structured assessment, CSIS, under the leadership of James A. Lewis, has based this review on the Cybersecurity Capability Maturity Model (CMM), originally applied in the 2016 Cybersecurity Report: Are We Ready in Latin America and the Caribbean? The CMM approaches cybersecurity through five dimensions of capacity and evaluates them along five stages of maturity for each of its 49 indicators. This document will complement the 2016 Cybersecurity Report by providing an overview of the experiences of these leading countries, describing how they have approached the problem of cybersecurity and how their policies have evolved. It serves as a useful guide to other countries as they develop their own national approaches to cybersecurity.

JEL codes: F52, O33, O38

Keywords: cybersecurity, cyber strategy, Critical National Infrastructure, cyber defense, trust online, legal frameworks, incident response, digital redundancy, resilience, cybercrime

Table of Contents

The dataset can be downloaded at: https://mydata.iadb.org/idb/dataset/a9yc-jpsa

Executive Summary

Access to the Internet and broadband services increase productivity, national income, and employment. Access to information catalyzes growth. However, these opportunities come with risk. Digital technologies are not mature and can be easily exploited by criminals and other antagonists. The question for public policy is how countries can manage risk without sacrificing opportunity. This study looks at the experience of four countries—Estonia, Israel, South Korea, and the United States—that are among the most advanced in cybersecurity, to see how they have answered this question. Each has made significant strides in cybersecurity, and useful lessons can be drawn from their experience.

There are wide disparities in size and wealth among these countries, but they share common experiences. Their cybersecurity policies are advanced because they have been quick to seize the economic opportunities offered by Internet and broadband services. In turn, each faces significant risks. The combination makes cybersecurity essential. Most nations do not face similar threats, but as the need for improved, more accessible Internet and broadband services increases, so does the need for better cybersecurity policies.

To provide a structured assessment, we have based our review on a Cybersecurity Capability Maturity Model (CMM) jointly developed by the Organization of American States, the Inter-American Development Bank, and Oxford University. Capability maturity models have wide applications in business and research. A maturity model assesses capabilities on a scale of complexity, completeness, and sophistication of national efforts. These dimensions range from initial efforts, which tend to be reactive and ad hoc, to strategic and dynamic efforts, where governments have made choices about policies and resource allocations. This CMM uses five levels of maturity: start-up, formative, established, strategic, and dynamic.[1] Each level indicates a higher degree of sophistication and capability. The model provides an extensive set of factors that enable the measurement of maturity in cybersecurity efforts.

Better cybersecurity requires creating strategies, rules, and institutions to make cyberspace more stable and secure in ways that enable economic growth and maximize the benefits of information technology. The maturity model looks at five categories of activity: policy and strategy; culture and society; education, training, and skills; legal and regulatory frameworks; and standards, organizations, and technologies.

While all are important, governments will need to prioritize them. Some recommended best practices are more implementable in the near term while other can take years. Each of the four nations was able to create a cybersecurity strategy in a matter of months, while each continues to struggle with workforce, cyber culture and standards despite years of effort. Some categories of action offer immediate returns

in terms of better cybersecurity. The experience of these four nations suggests three areas where a country may want to focus its initial efforts.

The first and foundational best practice for cybersecurity is the development of a national strategy. These strategies provide a policy framework under which countries can organize their cybersecurity efforts. The process of developing a strategy can also provide a mechanism for broad, cross-governmental coordination.

The second best practice is the creation of an organizational structure that clearly assigns responsibilities among government agencies for cybersecurity. One important aspect of this organizational best practice is the creation of a central coordinating authority. Cybersecurity is the responsibility of many agencies and at times can create overlapping requirements. Each of these countries created new, high-level entities, under the aegis of the Office of the President or the Prime Minister, to oversee cybersecurity. This is essential if a strategy is to be more than a piece of paper.

The third best practice is the adoption of appropriate laws and regulations for cybercrime, critical infrastructure, and data protection. The legal and regulatory framework is crucial for cybersecurity. Inadequate laws hamper government efforts, harm business, and encourage cybercrime. Legal and regulatory frameworks show the greatest divergence among the four countries. Each relies on a patchwork of existing law and new authorities. All four countries found it necessary to expand legal authorities to deal with cybercrime. Given the disparate applications of cybersecurity in so many different sectors of the economy, with different requirements and functions, this patchwork approach may make more sense than trying to draft a single, overarching law.

Strategy, organization, and rules are the first order of business. One lesson that can be drawn from the experience of the four countries is that it is better to take immediate action than to wait for the perfect strategy or the perfect law. No strategy is perfect. Organizations continue to evolve based on experience and drawing on best practices from other nations. The record of each country shows that iteration and evolution are part of national efforts to build better cybersecurity. Strategy in particular is best seen as the initiation of a process that will lead to better cybersecurity rather than the end of the discussion.

In each case, these nations made extensive efforts to be inclusive and involve the private sector. Estonia, Israel, and the United States made private sector participation a critical element of their cybersecurity efforts. How the private sector is involved varies from country to country, based on their political and business cultures. Some countries still retain ownership or control of public utilities. This changes the nature of the regulatory relationship. Others have privatized their public utilities and rely on different policy and regulatory tools to affect company behavior.

The term private sector can also be misleading. There are many different segments—critical infrastructure, international companies, and small and medium-sized enterprises. While there are commonalties in how governments work with companies on cybersecurity, each segment can also have differing requirements and must be engaged in ways tailored to best meet its cybersecurity needs. This adds complexity to any national effort, but a country can start with a simple, one-size-fits-all approach and then tailor it as needed.

Three of the countries—Israel, Korea, and the United States—have vibrant, competitive information technology (IT) sectors producing goods and services for a global market. This is useful but not essential for better national cybersecurity. Cybersecurity products and services are widely available in the global market. Countries can buy what they need, and the emphasis with respect to technology should be on understanding what cutting-edge technology is for cybersecurity and ensuring that there are processes in place to acquire it. Estonia shows that it is possible to achieve world-class cybersecurity without possessing a significant domestic IT industry. Importantly, companies in Israel and the United States are not national champions directly subsidized by the government. This introduces entrepreneurial and innovative aspects to company behavior. Companies move in the direction of the market, supported by the government, rather than the other way around. Countries can be tempted to adopt policies to build their own cybersecurity industry, but this can backfire if the result is reliance on domestic products that are not globally competitive and thus less able to protect.

Strategy, rules, and organization are immediate requirements, and it is possible to achieve immediate results. Other problems (e.g., workforce, education, and culture) are equally important, but long, sustained efforts will be required to make progress. All of the countries studied struggle with workforce issues. There is a global shortage of skill in cybersecurity. All four countries have programs to expand their cyber workforce, usually undertaken with universities and with the private sector.

Each country has emphasized the development of a cybersecurity culture. The best use primary and secondary school programs to inculcate good cyber habits. Others rely on awareness campaigns, but these seem to have varying effect.

All four countries have used international cooperation to build confidence, share best practices and information, and facilitate international efforts to build a stable cyber environment. This cooperation can range from CERT-to-CERT to high-level diplomatic activities, but is essential and provides nations with access to external informational and technical resources. The four countries have drawn on alliance relationships to strengthen their cyber defenses, and Estonia, the smallest, was the most active internationally.

Cybersecurity remains an evolving area of policy and practice. Each country is in its second or third iteration of a national approach. Best practices continue to evolve, guided by experience, new challenges, and greater understanding among policymakers.

With that in mind, the experiences of these countries serve as a useful guide to other countries as they develop their own national approaches to cybersecurity. These brief assessments describe how leading countries have approached the problem of cybersecurity and how their approaches have evolved. All share a goal of managing cyber risk to maximize the benefits of cyberspace for their citizens and businesses.

Notes

1. Cybersecurity Capability Maturity Model (CMM) Pilot, December 2014, *https://www.sbs.ox.ac.uk/*cybersecurity-capacity.

Introduction

Access to the Internet and broadband services has increased productivity, national income, and employment around the world. It is a catalyst for growth and plays a key part in any modern development strategy. However, access comes with risk. Digital technologies are not mature and can be exploited by criminals and other antagonists. Internet access creates public safety concerns that require government action. The greatest risks include financial crime and the stability of financial systems, the theft of confidential business and personal information, and the disruption of critical services. The question for public policy is how countries should manage risk without sacrificing opportunity.

This study looks at the experience of four countries that are among the most advanced in cybersecurity, as part of larger national efforts to take advantage of Internet access to improve economic performance and the delivery of government services. As they have moved forward, each has realized the importance of adequate cybersecurity. From their experience, useful lessons can be drawn for Latin American and Caribbean (LAC) countries to consider.

We define cyberspace as all of the devices connected over IP-based networks, not just the Internet. Cybersecurity requires creating strategies, rules, and institutions to make cyberspace more stable and secure. Cybersecurity seeks to protect information and data (intellectual property, communications, and personal information) and reduce the risk of disruption in the cyber environment and the critical infrastructures and services that depend on it.

We cannot rely on technology alone to address cybersecurity challenges. Each of these countries over time has developed and implemented complex strategies to reduce risk. In each country, development has been incremental, informed by experience and practice. From their experience, we can draw useful lessons on strategy, organization, policy, and regulation to increase the utility of Internet, and broadband access and to promote citizen security.

To provide a structured assessment, we have based our review on a “Cybersecurity Capability Maturity Model” jointly developed by the Organization of American States, the Inter-American Development Bank, and Oxford University. Capability maturity models, originally developed to streamline and improve software development, now have wide applications in business and research. Maturity, as defined for this purpose, refers to the degree of formality of behavior, practice, and processes in five capacity areas: (i) policy and strategy, (ii) culture and society, (iii) education, (iv) legal frameworks, and (v) technologies.

A maturity model assesses capabilities on a scale of complexity, completeness, and sophistication of national efforts. These, range from initial efforts, which tend to be reactive and ad hoc, to strategic and dynamic efforts, where governments have made choices about policies and resource allocations. These decisions can be altered or modified in response to changing circumstances. This Cybersecurity

Capability Maturity Model (CMM) uses five levels of maturity: startup, formative, established, strategic, and dynamic.[1] Each level indicates a degree of sophistication and capability. The lowest level implies an ad hoc level of capacity, while the highest indicates a dynamic approach capable of responding quickly to new requirements.

Deciding where a country falls on these levels depends on identifying specific actions it has taken and attributes that it has. In the case of cybersecurity marketplace development, for example, the CMM ranks maturity using a progressive scale of indicators, from having little or no access to technology to producing information technology for the global market. Each category has specific indicators that can be used to assess maturity.[2]

In each case, the development of national cybersecurity efforts was an iterative process, starting with existing institutions and laws and, over time, modifying or expanding them as necessary and creating new policies, regulations, laws, and institutions. Each of the countries continues to modify and adjust its national approach to cybersecurity in light of its experience.

An assessment of the four countries reviewed suggests that they all fall somewhere between "strategic" and "dynamic" in their cybersecurity capabilities. None is completely dynamic. This is in many ways a reflection of the slowness of democratic processes when it comes to amending laws or creating new organizations, but all have considered the requirements of national cybersecurity and made choices. In contrast, most countries in the LAC region are at the formative level. We offer this study to guide national efforts to improve cybersecurity capacity.

It is worth noting that each of the countries under review faces serious military opponents in cyberspace. These threats to national security and public safety create powerful incentives that explain much of the attention paid by the four countries to cybersecurity. The threat environment is, fortunately, very different for the LAC countries, but this does not mean that there is no need for action. Governments ignore cybersecurity at their peril, and inattention will inevitably damage prospects for development and growth.

Notes

1. Cybersecurity Capability Maturity Model (CMM) Pilot, December 2014, **https://www.sbs.ox.ac.uk/cybersecurity-capacity**
2. Cybersecurity Capability Maturity Model (CMM) V1.2, pps.8–41, **https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version1.2.pdf**

.ee

Republic of Estonia

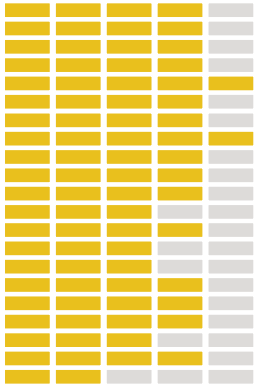
Policy and Strategy

Culture and Society

Education

Legal Frameworks

Technologies



Main Cybersecurity Challenges

After regaining independence from the Soviet Union in 1991, Estonia had limited resources to meet high public expectations for modernized infrastructure and better delivery of government services. The institutional vacuum after independence gave Estonia a unique opportunity to create innovative technologies and practices. With the freedom to design its own government, Estonia facilitated early adoption of information and communication technologies (ICT), and the government readily embraced electronic service delivery. Of the four countries reviewed in this publication, Estonia comes closest to having a "dynamic" approach to cybersecurity. Its political leaders have made cybersecurity a hallmark of Estonian foreign policy.

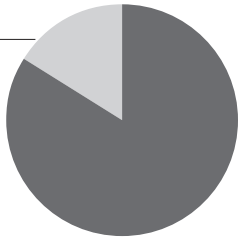
Today, 25 years after independence, Estonia's geographic proximity to Russia continues to dominate its security considerations, including in cyberspace.

Adopted in 2008, Estonia's first cybersecurity strategy was shaped by the cyber attacks launched in 2007,[1] following the removal of a large, Soviet-era statue of a Russian soldier from the center of Tallinn to a remote suburb. Since then, Estonia's strong digital economy and its proximity to cybercrime hubs in Eastern Europe make it a target for cyber theft and fraud. Estonia also uses ICT to generate economic growth. It encourages foreign companies to establish a digital presence in Estonia by offering them online processing of administrative government services, including tax filings. Estonia's Internet economy involves cross-border data flows, often relying on ICT infrastructure based outside of the country. The Estonian government tracks these ICT interdependencies to prepare backup systems and redundancies in case of disruption from cyber attack or natural disaster.

TOTAL POPULATION IN THE COUNTRY	**1,314,545**
Mobile cellular subscriptions	2,062,864
Internet users	1,106,846

Internet penetration

84%



Source: World Bank Development Indicators (2014). Available at http://databank.worldbank.org/data/reports.aspx?source=2&country=USA&series=&period=.

Policy and Strategy

Official National Cybersecurity Strategy

- Strategy development
- Organization
- Content

Cyber Defense Consideration

- Strategy
- Organization
- Coordination

Culture and Society

Cybersecurity Mind-Set

- Government
- Private Sector
- Society

Cybersecurity Awareness

- Awareness raising

Confidence and Trust on the Internet

- Trust in use of online services
- Trust in e-government
- Trust in e-commerce

Online Privacy

- Privacy standards
- Employee privacy

Education

National Availability of Cyber Education and Training

- Education
- Training

National Development of Cybersecurity Education

- National development of cybersecurity education

Training and Educational initiatives

- Training employees in cybersecurity

Corporate Governance, Knowledge and Standards

- Private and state-owned companies' understanding

Legal Frameworks

Cybersecurity Legal Frameworks

- Legislative frameworks for ICT security
- Privacy, data protection and other human rights
- Substantive cybercrime law
- Procedural cybercrime law

Legal investigation

- Law enforcement
- Prosecution services
- Courts

Responsible Reporting

- Responsible disclosure

Technologies

Adherence to Standards

- Implementation of Standards
- Procurement
- Software development

Cyber Security Coordinating Organizations

- Command and control center
- Incident response capacity

Incident Response

- Identification and designation
- Organization
- Coordination

National Infrastructure Resilience

- Infrastructure technology
- National resilience

Critical National Infrastructure Protection

- Identification
- Organization
- Response planning
- Coordination
- Risk management

Crisis Management

- Planning
- Evaluation

Digital Redundancy

- Planning
- Organization

Cybersecurity Marketplace

- Cybersecurity technologies
- Cybercrime insurance

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Cybersecurity Policy and Strategy

Dynamic

Estonia was one of the first countries to develop a national cybersecurity strategy. The Estonian government updated its 2008 strategy in 2014, issuing a revised version to cover the period 2014–2017. The strategy is the basic planning document for Estonian cybersecurity and an element of Estonia's larger national security strategy. The new strategy builds on its predecessor but reevaluates its approach in light of changes in the threat environment. The 2014–2017 Estonian cybersecurity strategy has several objectives, including:

- Invigorating a comprehensive, all-of-government approach to cybersecurity;
- Creating a very high level of cybersecurity competence and awareness in agencies, companies, and among the public;
- Strengthening regulation to secure information systems; and
- Supporting efforts to build international cooperation in cybersecurity.

The strategy focuses on ensuring the provision of vital services, enhancing Estonia's ability to combat cybercrime, and improving its national defense capability. While separate agencies are assigned this task at the national level, Estonia's overall approach seeks to avoid compartmentalization of responsibilities to ensure a coordinated response in the event of a significant national cyber incident. Among the tasks identified in the strategy are developing the legal framework, improving international cooperation, and expanding the number of experts and solutions for cybersecurity.

Estonia made significant organizational changes in support of its cybersecurity strategy. In 2009, a Cybersecurity Council, tasked with supporting inter-agency cooperation and overseeing implementation of the strategy, was added to the Security Committee of the Government of the Republic (a ministerial body). The Estonian Information System Authority (Riigi Infosüsteemi Amet, or RIA), which was given additional powers and resources for the protection of government networks. Within the RIA, Estonia created a "Department of Critical Information Infrastructure Protection."

The RIA undertook a critical infrastructure-mapping project to identify vital services that rely on cyber means and formed a commission to promote public-private cooperation. The cybercrime units of Police and Border Guard Board (PBGB) were merged in 2012. A Cyber Defense Unit (CDU) was created in 2011 as part of the Estonian Defense League, a volunteer home-defense organization.[2] The CDU brings private sector expertise into the government domain.

The Cybersecurity Council monitors the overall implementation of Estonia's cybersecurity strategy. It is supported by the Ministry of Economic Affairs and Communications, which coordinates the implementation of cybersecurity policy among government agencies, civil society, companies, and educational institutions. All agencies involved in cybersecurity[3] provide an annual report to the Ministry of Economic Affairs and Communications on measures they have adopted and their performance.

Estonia's Cyber Emergency Response Team (CERT-EE) manages cyber incident response. CERT-EE prioritizes cases according to four principles:[4] (i) the number of affected users, (ii) the seriousness of

the incident, (iii) the target of an attack and the attack's point of origin; and (iv) the resources required to handle the incident.

CERT-EE operates under the framework of the RIA, which monitors vulnerabilities in information systems underlying vital services and critical infrastructure. As such, it maintains the "X-Road" framework. X-Road is a platform for secure information exchange between government agencies and the general population.[5] Initiated in 2001 to connect government databases, the X-Road project now provides secure communication services to accredited private sector actors.

Estonia has held regular national cybersecurity exercises in 2010, 2012, and 2015. The cyber range established by Estonia for training purposes is also available for use by universities. Strengthening national expertise through cooperation with international allies and partners from the private sector is not only a measure of confidence building, but also cost reduction. Estonia's concept of cybersecurity also encompasses safeguarding the online exercise of fundamental rights and citizens' freedom.

D1-1 Documented or Official National Cybersecurity Strategy	
Estonia updated its cyber strategy in 2014 based on the evaluated impact of its first planning document from 2008. The document is designed for a specific timeframe (2014–2017), with annual performance ratings and respective adjustments.	http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014–2017_public_version.pdf.
D1-2 Cyber Defense Consideration	
Regular exercises with NATO allies form a core component of the 2014 strategy. The creation of the Cyber Defense Unit within the Estonian Defense League has strengthened civil-military cooperation on cyber defense.	https://ccdcoe.org/multimedia/cyber-defence-unit-estonian-defence-league-legal-policy-and-organisational-analysis-0.html.

Cyber Culture and Society

Strategic

Estonia prides itself on its advanced e-government services and its tech-savvy population. Estonia is a leader in e-governance, including the digital authentication of identity. Its electronic ID card is the key to accessing Estonia's e-government services. Through the digital signature and identity authentication certificate saved on the card, citizens gain access to the systems for Internet voting, online tax returns, e-prescriptions, and online health records.[6] The ID also serves as the repository of e-tickets for public transportation. With the implementation of Estonia's e-residency program, signing documents online, establishing a company in Estonia over the Internet, managing it remotely, and filing taxes over the Internet have become possible for anyone worldwide.[7]

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Estonia was an early adopter of Internet voting, beginning with the parliamentary election of 2007. Participation rates have continuously grown over the years, reaching a record high of 30.5 percent of voters casting their ballot online in 2015.[8] I-voting has become a stocktaking measure for the degree of confidence that citizens place in cybersecurity.[9] Estonia relies on government-supported private sector initiatives to advance its cybersecurity initiatives. The awareness campaigns and trainings organized by the Look@theWorld Foundation, a support network established by Estonian and international service providers, have been a key driver in the promotion of the secure use of ICT devices. As part of its Computer Security 2009 project, 400,000 individuals[10] were trained on how to protect themselves from identity theft.[11] In 2014, a follow-up initiative was launched with similar training objectives for users of mobile smart devices and digital signatures.[12] The goal is to reach 300,000 individuals, approximately 70 percent of mobile smart device users in Estonia, by 2017. According to the 2015 cybersecurity survey conducted by the European Commission, 47 percent of Estonian respondents said they felt well informed about the risks of cybercrime.[13]

Together with 26 other nations, Estonia is part of the Freedom Online Coalition, which advocates the "free expression, association, assembly and privacy online." The coalition coordinates national positions and joint statements.[14] The uninhibited exercise of these freedoms inspired many of electronic services provided by the Estonian government.

D2–1 Cybersecurity Mindset	
The 2007 cyber attacks have generated a collective awareness of the potential vulnerabilities that Estonia's interconnected society and economy face.	
D2–2 Cybersecurity Awareness	
Concerted training programs in cooperation with private sector initiatives have been implemented and are revised periodically to reflect technological changes.	http://www.vaatamaailma.ee/en. http://www.vaatamaailma.ee/en/nutikaitse.
D2–3 Confidence and Trust on the Internet	
The X-Road framework provides a government-secured ecosystem for the data exchange between citizens, government agencies, and third-party service providers.	https://www.ria.ee/public/x_tee/xRoadOverview.pdf.
D2–4 Privacy Online	
Privacy is an integral part of Estonia's cyber strategy that promotes and protects the exercise of civil rights online. The Personal Data Protection Act of 1996 was amended in 2010 to meet EU standards.	http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete+kaitse+seadus.

Cybersecurity Education, Training, and Skills

Strategic

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Estonia has created educational programs at the elementary, middle school, and college levels. The Information Technology Foundation for Education (HITSA) functions as the primary source of training and awareness campaigns in Estonia, beginning its training programs with pre-school age children. HITSA held its first cyber defense competition for secondary school students in June 2015 with the goal of inspiring the next generation of cybersecurity professionals.[15] The top five participants were invited to tours of the Ministry of Defense, NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), the CDU, and the Estonian Information System Authority. Over the summer, HITSA also hosted the first cybersecurity summer school with 70 international participants and faculty from, among others, the University of California, Berkley, Oxford University, and University College London.[16]

In higher education, the Estonian Information Technology College will launch a new English-language degree program in cybersecurity engineering.[17] The new undergraduate program complements existing master's-level programs. Since 2009, the Tallinn University of Technology and the University of Tartu have offered a joint MA program in cybersecurity, admitting about 50 students every year. In 2014, the Tallinn University of Technology, in collaboration with the Estonian Centre 2CENTRE on Cybercrime, launched an MA program in digital forensics. The 2CENTRE on Cybercrime is part of a larger Centers of Excellence Network organized by the European Union to train professionals to fight cybercrime.

In 2002, the Estonian government, with support from United Nations Development Programme and the Open Society Institute, created an independent nongovernmental organization, thee-Governance Academy (EGA).[18] The EGA works to share Estonia's experience in developing e-government, e-democracy, and ICT education systems.

Despite these efforts, Estonia faces shortfalls in its cyber workforce. A survey of ICT labor market conditions requested by the European Commission projects the labor force in the Estonian ICT sector to increase to 24,000 by 2015 (up from 23,000 in 2012).[19] Despite steady growth in these numbers since 2001, the general shortage of ICT professionals, when measured against demand, has led to a considerable increase in salaries. Many students leave without finishing their degree in order to take high-paying jobs in the private sector.

D3-1 National Availability of Cyber Education and Training

The Information Technology Foundation for Education, as the cybersecurity education-facilitating institution on the national level, begins its programs at the pre-school age. Elementary, middle, and high school curricula contain cybersecurity modules.	http://www.hitsa.ee/it-education/educational-programmes.

D3–2 National Development of Cybersecurity Education

Estonia recognizes the need to further internationalize its higher education efforts in cybersecurity and actively seeks to hire expert faculty from abroad. The current shortage of trained IT security professionals prompts a significant number of students to join the labor market without finishing their degree.

http://ec.europa.eu/DocsRoom/documents/4568/attachments/1/translations/en/renditions/native.

D3–3 Training and Educational Initiatives in Public and Private Sector

An increasing number of degree programs dedicated to cybersecurity exist at the graduate and undergraduate levels. Efforts to share Estonia's experience in developing e-government, e-democracy, and ICT education systems with developing countries help systematize achievements.

http://www.hitsa.ee/about-us/news/article-2

http://www.ega.ee/.

D3–4 Corporate Governance, Knowledge and Standards

The Estonian government, with the electronic ID, digital signatures, and the X-Road system, has established a common security infrastructure, also for use in the private sector.

Benefits of harmonization and the cost-saving rationale of companies have led to the early adoption of these measures.

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Legal and Regulatory Frameworks

Strategic

Estonia has developed an extensive set of legislation and regulation for cybersecurity. The most important of these is the Emergency Act of 2009.[20] The Act states that critical infrastructure and its implementation in the ICT sector are governed by the Regulation on Security Measures for Information Systems of Vital Services and Related Information Assets (2013).[21] This regulation requires vital service providers to report cyber incidents and submit reports to the Estonian Information System Authority after integrity of the system is restored.

The State Secrets and Classified Information of Foreign States Act of 2007 calls for an annual assessment of the digital storage security of government documents classified as "top secret" and "secret."[22] The Electronic Communications Act 2004 (amended in 2011)[23] authorizes the Technical Surveillance Authority of Estonia to request ICT service providers to conduct security assessments of their own systems. The processing of correspondence and personal information is governed by the

Personal Data Protection Act 1996 (last amended in 2010).[24] The Act implements EU data protection standards, distinguishes between "personal data" and "sensitive personal data", and places "sensitive personal data" under extended protection.

After 2007, the Estonian authorities decided that the cybercrime provisions in the national Penal Code were inadequate for dealing with coordinated cyber actions that did not clearly seek financial gain. A series of amendments to the Estonian Penal Code have since expanded the spectrum of punishable acts.

Specifically, the Estonian legislature has extended coverage to the illegal alteration, deletion, damaging or blocking of data, interference with or hindering of operation of computer systems, the dissemination of malicious tools, the preparation of cybercrime, and the unlawful use of computer systems, codifying significantly higher maximum penalties for operations directed against vital services or infrastructure.[25] Further, changes to the penal code have broadened the scope of acts of terrorism to include "interference with computer data or hindrance of operation of computer systems, as well as threatening such acts, if committed for the purpose of forcing the state or an international organization to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organization, or to seriously terrorize the population."[26]

D4-1: Cybersecurity Legal Frameworks	
The Regulation on Security Measures for Information Systems of Vital Services and Related Information Assets of 2013 defines critical information infrastructure in relation to the 2009 Emergency Act. Tightening of the Estonian Penal Code introduced a range of new cybersecurity-specific statutory offenses.	https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf. https://www.riigiteataja.ee/en/eli/522012015002/consolide.
D4-2: Legal Investigation	
The Estonian Public Prosecutor's Office is responsible for investigating cases under the Penal Code. International mutual legal assistance treaties exist but may prove to be of limited practical value in times of tension.	http://www.prokuratuur.ee/en.
D4-3: Responsible Reporting	
Vital service providers, under the Regulation of Security Measures for Information Systems of Vital Services and Related Information Assets, are required to report cyber incidents and update the Estonian Information System Authority after integrity of the system is restored.	https://www.ria.ee/en/.

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Standards, Organizations, and Technologies

Strategic

Estonia, given its small size and location, has made international cooperation a core part of its cybersecurity strategy. Estonia uses international cooperation to improve its own security and to increase its international influence. In addition to regional partnerships with the Baltic and Nordic states, Estonia actively participates within the frameworks of NATO, the European Union, the UN Group of Government Experts, and the Organization for Security and Cooperation in Europe (OSCE). A key component of Estonian cybersecurity planning is strengthening cooperation with NATO, not least through hosting the alliance's cyber exercises and forums. Estonia has hosted numerous international cyber exercises, including the annual NATO Locked Shields and the NATO Cyber Coalition defense exercises since 2013, to prepare for the kind of attacks experienced in 2007.[27] One of the first activities launched under the OAS cybersecurity Initiative, the Estonian Computer Emergency Response Team in May 2015 organized a four-day training for government officials from Costa Rica, Guyana, Jamaica, Nicaragua, Panama, Paraguay, and Uruguay to share its experience in developing and managing national CIRTs.[28]

To avoid the problems created by the 2007 denial of service attacks against government websites, the 2014–2017 Cyber Strategy envisions virtual embassies hosted in a public cloud that relies on servers based in Estonia and data centers in friendly countries. This will provide alternative avenues of access and add an additional layer of security.[29] Virtual embassies are intended to ensure e-services are maintained even in the event of a physical attack on Estonia that might disrupt the functioning of government in the traditional sense. The concept of the "digital continuity of the state"[30] introduces this idea of redundancy for government services.

Estonia adopted its own IT security standard modeled on the IT-Grundschutz ("IT Baseline Protection Manual") developed by the Federal Office for Information Security of Germany (BSI). Compulsory for the public sector since 2008, the ISKE standard employs a three-level assessment for an entity's security requirements (high, medium, low). The standard seeks to balance confidentiality, integrity, and the availability of data.[31]

D5-1: Adherence to standards

Estonia adopted its own IT security standard ISKE, modeled on the IT-Grundschutz ("IT Baseline Protection") developed by Germany. Since 2008 implementation has been binding for the public sector. ISKE ranks an organization's security requirements based on a three-tier system (high, medium, low).	https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf.

D5-2: Cybersecurity Coordinating Organizations

The Cybersecurity Council monitors the implementation of the cybersecurity strategy. Support comes from the Ministry of Economic Affairs and Communications that guides cybersecurity policy and coordinates its execution among government agencies, civil society representatives, companies, and educational institutions. Responsibility for protecting government networks rests with the Estonian Information System Authority (RIA).

https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014–2017_public_version.pdf.

D5-3: Incident Response

The Cyber Emergency Response Team of Estonia (CERT-EE), operating under RIA, manages cyber incident response. RIA directly monitors the information systems underlying vital services and critical infrastructure.

https://www.ria.ee/cert-estonia/.

D5-4: National Infrastructure Resilience

Backup alternatives exist for e-services and vital information systems.

D5-5: Critical National Infrastructure (CNI) Protection

RIA has mapped critical infrastructure and vital services that rely on information systems for their operation and delivery. Cross-border interdependencies have been reduced.

https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014–2017_public_version.pdf.

D5-6: Crisis Management

CERT-EE assigns response priorities based on the four principles of: the number of affected users; the type of an incident; the target of an attack as well as the attack's point of origin; resources required to handle the incident.

https://www.ria.ee/cert-estonia/.

D5-7: Digital Redundancy

Estonia plans to maintain virtual embassies on servers based in Estonia and data centers in friendly countries. Hosted in public clouds, these virtual embassies provide alternative access routes, adding an additional layer of security. Virtual embassies are designed to ensure that essential e-services remain available, even in the event of a physical attack on Estonia that might disrupt the functioning of government in the traditional sense.

https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf.

D5–8: Cybersecurity marketplace

The ICT sector is estimated to be among the fastest-growing industries in Estonia through 2022. Estonia's e-residency program creates a climate conducive to foreign investment, allowing investors worldwide to establish a company in Estonia over the Internet, manage it remotely, and file taxes over the Internet. However, three-quarters of Estonian CEOs have voiced concerns about the government's effectiveness in training a cyber-ready workforce.

https://e-estonia.com/e-residents/about/.

http://euskillspanorama.cedefop.europa.eu/App_Controls/Documents/ShowDocument.aspx?documentid=127&.

Notes

1. Ministry of Defense of the Republic of Estonia, cybersecurity Strategy of Estonia 2008–2013, 2008, **http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf.**
2. Kadri kaska, Anna-Maria Osula, LTC Jan Stinissen, "The Cyber Defence Unit of the Estonian Defence League," NATO CCD CoE, 2013, **https://ccdcoe.org/multimedia/cyber-defence-unit-estonian-defence-league-legal-policy-and-organisational-analysis-0.html.**
3. These agencies include the Ministry of Defense, the Information System Authority, the Ministry of Justice, the Police and Border Guard Board, the Government Office, the Ministry of Foreign Affairs, the Ministry of the Interior, and the Ministry of Education and Research.
4. Republic of Estonia Information System Authority (RIA), "About CERT Estonia," January 13, 2014, **https://www.ria.ee/cert-estonia/.**
5. RIA, "X-Road Overview," accessed October 9, 2015, **https://www.ria.ee/public/x_tee/xRoadOverview.pdf.**
6. "e-Estonia," estonia.eu, **http://estonia.eu/about-estonia/economy-a-it/e-estonia.html.**
7. "What is e-Residency?", e-estonia.com, accessed October 9, 2015, **https://e-estonia.com/e-residents/about/.**
8. National Election Committee of Estonia, "Statistics about Internet Voting in Estonia," accessed October 9, 2015 **http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics.**
9. On security aspects of Estonia's I-voting system see Drew Springall, Travis Finkenauer, et al., "Security Analysis of the Estonian Internet Voting System," November 2014, **https://estoniaevoting.org/findings/paper/.**
10. The World Bank estimates Estonia's population at 1.314 million (2014). **http://data.worldbank.org/country/estonia.**
11. Look@World Foundation, "Past Milestones," accessed October 9, 2015, **http://www.vaatamaailma.ee/en/.**
12. Look@World Foundation, "Estonia Puts Focus on Smart Device Security," accessed October 9, 2015, **http://www.vaatamaailma.ee/en/nutikaitse.**
13. Special Eurobarometer 423, "Cybersecurity Report," survey conducted by TNS Opinion & Social at the request of the European Commission, Directorate-General for Home Affairs, February 2015, 41–2, **http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf.**
14. Freedom Online Coalition, "Overview of the Freedom Online Coalition's Work and Vision to Advance Internet Freedom Globally," July 2015, **https://www.freedomonlinecoalition.com/wp-content/uploads/2015/07/Freedom-Online-Coalition-Basic-facts-July-2015.pdf.**
15. "First Cyber Defence Competition for Schoolchildren," studyITin.ee, accessed October 9, 2015, **http://studyitin.ee/en/estonian.**
16. nformation Technology Foundation for Education, "Estonia Hosts the First International cybersecurity Summer School," July 10, 2015, **http://www.hitsa.ee/about-us/news/estonia-hosts-the-first-c3s.**
17. Information Technology Foundation for Education, "Estonian IT College is Opening a New Curriculum - cybersecurity Engineering," June 1, 2015, **http://www.hitsa.ee/about-us/news/article-2.**
18. Estonian e-Governance Academy, **http://www.ega.ee/.**
19. empirica, "e-Skills in Europe: Estonia Country Report," requested by the European Commission, January 2014, 7, **http://ec.europa.eu/DocsRoom/documents/4568/attachments/1/translations/en/renditions/native.**
20. Emergency Act, Republic of Estonia, RT I 2009, 39, 262, as last amended by RT I, 30.06.2015, 4, **https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/504092015012/consolide.**

21. Regulation no. 43 of March 14, 2013, Republic of Estonia, Security Measures for Information Systems of Vital services and Related Information Assets, **https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf.**

22. State Secrets and Classified Information of Foreign States Act, Republic of Estonia, RT I 2007, 16, 77, as last amended by RT I, 22.12.2011, 2, **https://www.riigiteataja.ee/en/eli/515112013009/consolide.**

23. Electronic Communications Act, RT I 2004, 87, 593, Republic of Estonia, as last amended by RT I, 25.03.2011, 1, **http://www.konkurentsiamet.ee/public/Electronic_Communications_Act_2011.pdf.**

24. Personal Data Protection Act, Republic of Estonia, RT I 2007, 24, 127, as last amended by RT I, 30.12.2010, 2, **https://www.riigiteataja.ee/en/eli/512112013011/consolide.**

25. Penal Code, Republic of Estonia, RT I 2001, 61, 364, as last amended by RT I, 26.02.2014, 1, paragraphs 206, 207, 208, 216, 217, **http://www.wipo.int/wipolex/en/text.jsp?file_id=333555.**

26. Ibid. paragraph 237 (1).

27. NATO CCD CoE, Centre, "Estonian Defense League Sign Cooperation Agreement," February 12, 2015, **https://ccdcoe.org/centre-estonian-defence-league-sign-cooperation-agreement.html.**

28. Cybersecurity Capacity Portal, University of Oxford, "OAS and Estonia Promote Exchange of Best Practices on Cybersecurity," May 5, 2015, **https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/oas-and-estonia-promote-exchange-best-practices-cyber-security.**

29. Ministry of Economic Affairs and Communications of Estonia and Microsoft Corporation, "Implementation of the Virtual Data Embassy Solution," 2015, **https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf.**

30. cybersecurity Strategy 2014–2017, p.9.

31. RIA, "Estonian Security System Overview," 2012, **https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf.**

.il

State of Israel

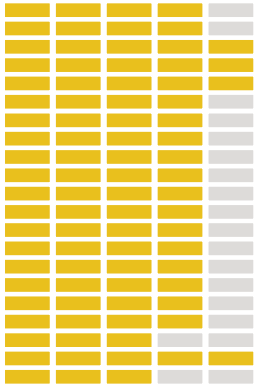
Policy and Strategy

Culture and Society

Education

Legal Frameworks

Technologies



Main Cybersecurity Challenges

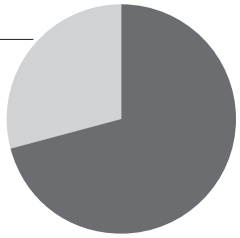
Israel's cyber defense apparatus is one of the best in the world. A comparative study of 23 developed countries ranked Israel as best in cyber defense, along with Sweden and Finland.[1] Despite this, both strategies and organization continue to evolve in Israel. Each day, hostile groups at the state and non-state levels test Israel's cyber defenses. Government agencies and critical infrastructure—particularly the electricity sector—are regularly targeted.

Israel's cybersecurity policies have shifted in response to an increased reliance on cyberspace for political, military, and economic activities. This reliance means that without adequate cybersecurity, a determined adversary could disrupt key strategic targets without confronting Israel with a conventional military. Israel determined that the existing civil-military organizational structures, responsibilities, and regulations for protecting computerized systems—which were highly compartmentalized—were inadequate to enable a comprehensive defense in cyberspace.[2]

TOTAL POPULATION IN THE COUNTRY	**8,215,700**
Mobile cellular subscriptions	9,982,075
Internet users	5,874,225

Internet penetration

71%



Source: World Bank Development Indicators (2014). Available at http://databank.worldbank.org/data/reports.aspx?source=2&country=USA&series=&period=.

Policy and Strategy

Official National Cybersecurity Strategy

- Strategy development
- Organization
- Content

Cyber Defense Consideration

- Strategy
- Organization
- Coordination

Culture and Society

Cybersecurity Mind-Set

- Government
- Private Sector
- Society

Cybersecurity Awareness

- Awareness raising

Confidence and Trust on the Internet

- Trust in use of online services
- Trust in e-government
- Trust in e-commerce

Online Privacy

- Privacy standards
- Employee privacy

Education

National Availability of Cyber Education and Training

- Education
- Training

National Development of Cybersecurity Education

- National development of cybersecurity education

Training and Educational initiatives

- Training employees in cybersecurity

Corporate Governance, Knowledge and Standards

- Private and state-owned companies' understanding

Legal Frameworks

Cybersecurity Legal Frameworks

- Legislative frameworks for ICT security
- Privacy, data protection and other human rights
- Substantive cybercrime law
- Procedural cybercrime law

Legal investigation

- Law enforcement
- Prosecution services
- Courts

Responsible Reporting

- Responsible disclosure

Technologies

Adherence to Standards

- Implementation of Standards
- Procurement
- Software development

Cyber Security Coordinating Organizations

- Command and control center
- Incident response capacity

Incident Response

- Identification and designation
- Organization
- Coordination

National Infrastructure Resilience

- Infrastructure technology
- National resilience

Critical National Infrastructure Protection

- Identification
- Organization
- Response planning
- Coordination
- Risk management

Crisis Management

- Planning
- Evaluation

Digital Redundancy

- Planning
- Organization

Cybersecurity Marketplace

- Cybersecurity technologies
- Cybercrime insurance

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Cybersecurity Policy and Strategy

Strategic

Israel was one of the first countries in the world to recognize the importance of defending its critical computerized systems. In 1997, Tehila—Israel's e-government project—was launched with the goal of protecting the connection of government offices to the Internet and providing secure hosting for government sites. Tehila aims to improve online interaction between the government and its citizens. It has the dual function of serving as the Internet service provider (ISP) for government ministries and hosting the government's websites and services. The Tehila infrastructure has withstood distributed denial-of-service attack (DDoS) attacks, some larger than the 2007 attack against Estonia.[3]

In 2002, Israel passed National Security Ministerial Committee Resolution 84/B on the responsibility for protecting computerized systems in the State of Israel. Resolution 84/B became the de facto national civilian cyber defense policy, providing the initial framework for national critical computer systems (CCS).[4] The framework also identified the areas of responsibility for defining critical computerized infrastructure and establishing the National Information Security Authority (NISA), which regulates and advises critical infrastructures in the field of information security.

In 2010, because of increased threats in the cyber domain, the prime minister directed the creation of the National Cyber Initiative, a task force to formulate national plans to put Israel among "the top five countries leading the cyber field."[5] The initiative, headed by the chairman of the National Council for Research and Development, developed a strategy for preparedness in cyberspace and for cooperation among its economic, academic, and national security components.

The Israeli National Cyber Bureau (INCB), established in 2010, is responsible for coordinating national and international exercises. It is also responsible for assembling an intelligence overview from all intelligence bodies and providing a national situation status regarding cybersecurity. The INCB is the result of the goals laid out in the National Cyber Initiative of 2010. The seven key recommendations of that initiative were:

1. Improve education, from basic best practice and to advanced interdisciplinary R&D
2. Develop a knowledge and R&D infrastructure
3. Create a statewide "protective shield" based on the products of domestic R&D, while addressing privacy concerns
4. Develop national operational capabilities in cyberspace
5. Upgrade defense by combining technical and non-technical legislative measures and participating in international initiatives, especially with the Council of Europe Convention on Cybercrime, to promote cyber defense
6. Deploy unique technologies, developed domestically, with the government encouraging local procurement
7. Build a national agency for comprehensive cyber policy in Israel

The INCB is charged with promoting three central areas in the cyber field in Israel:

1. Advancing defense and building national strength in the cyber field
2. Building up Israel as a center of information technology
3. Encouraging cooperation among academia, industry, the private sector, government offices, and the security community

The INCB, which reports directly to the prime minister, brought a new interdisciplinary thrust to the direction and character of Israel's cybersecurity policy debates and capabilities. The INCB was tasked with advising the prime minister, the government, and its committees (excluding military and foreign relations) to consolidate, guide, and inform the government's initiatives and efforts in devising national cyber policy. The INCB also provides national cyber threat estimates, promotes R&D and industry efforts, increases public awareness on cybersecurity issues, and facilitates domestic and international cooperation on cyber issues.

The most recent action was the creation of a national cyber defense authority in February 2015 by the Prime Minister's Office. This followed a year of bureaucratic infighting over the question of who would be responsible for the new agency. In the end, the prime minister decided not to task Israel's domestic security agency, Shin Bet, with this responsibility.[6] Shin Bet has traditionally been in charge of protecting state agencies and critical infrastructure, such as electricity, water, and financial institutions, from cyberattacks and intrusions. Some viewed this decision as prioritizing privacy over security interests.

The National Cyber Defense Authority will have overall responsibility for cyber defense. The authority's offices will be located in Tel Aviv and Beer-Sheba. The authority will act in concert with the INCB, which will continue to set national policy. The new authority and the bureau will constitute a single national cyber directorate. The INCB was appropriated an ILS 2.5 billion budget for the next five years—about ILS 500 million (US$130 million) a year.[7] The Cyber Defense Authority will develop a comprehensive response against cyber attacks, including dealing with threats and events in real time. Its responsibilities include not just critical infrastructure and government networks, but also large commercial networks not previously considered critical infrastructure, such as airlines and food processing companies. The authority will also operate an assistance center—a Cyber Event Readiness Team (CERT)—to strengthen the resilience of organizations and sectors in the economy.

The Israeli Defense Forces (IDF) will operate in conjunction with the new Cyber Defense Authority but will be responsible for military aspects of cyber defense. In June 2015, the IDF spokesperson announced that in light of substantial challenges facing the IDF in the cyber realm, the chief of staff had decided to establish a cyber command to lead the military's operational activities. The IDF plans to establish this command in two years. The new command will examine ways to enhance military operational effectiveness in the cyber realm, better utilizing "the technological and human advantages already existing in Israel."[8]

D1–1 National Cybersecurity Strategy	
The National Cyber Initiative was launched in 2010, which led to the establishment of the Israeli National Cyber Bureau (INCB)	http://sectech.tau.ac.il/cyberconference/index.php/israeli-national-cyber-bureau
D1–2 Cyber Defense Consideration	
The National Cyber Defense Authority was launched in February 2015 to work in concert with INCB.	http://mfa.gov.il/MFA/PressRoom/2015/Pages/Cabinet-approves-establishment-of-National-Cyber-Authority-15-Feb-2015.aspx

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Cyber Culture and Society

Dynamic

Israel's defense needs and limited resources have helped to create a national focus on technology.[9] Its vibrant democracy and small size have fostered an intense digital culture. According to 2013 ITU statistics, 70.8 percent of the population in Israel are Internet users.[10] According to a study done by Hebrew University in May 2014, 81 percent of Israelis aged 12 and over go online; two-thirds go online several times a day.[11]

High Internet penetration is reflected in Israel's entrepreneurial private sector for cybersecurity, one of the fastest growing in the world. Over the past five years, the number of Israeli cybersecurity companies has doubled, to 300.[12] This growth can be attributed largely to its wealth of engineers. These engineers come mostly from two places. First, many are former employees of the 280 high-tech development centers in Israel owned by foreign multinationals. Second, thousands of engineers who leave the IDF each year bring skills suited to the burgeoning cybersecurity industry in Israel.

The INCB says that Israel is responsible for more exports of cyber-related products and services than all other nations combined, apart from the United States.[13] In 2014, Israeli cybersecurity startups exported US$3 billion in cyber goods, second only to the United States, and constituted 5 percent of the global market. At least one-third of Israeli exports are associated with ICT, while only about 7 percent of Israel's human capital works in the ICT sector.[14] In 2013, Israeli startups raised US$165 million in investment funding, or 11 percent of global capital invested in cybersecurity. Moreover, almost 15 percent of all the firms worldwide attracting cyber-related investment are Israeli-owned.[15]

Privacy is considered a fundamental human right under Israeli law and is guaranteed by its Basic Law."[16] The Privacy Protection Act of 1981 (PPA) protects privacy. The PPA, a product of several expert committees in the 1970s and early 1980s, was one of the first privacy laws of its kind in the world.[17] The Israeli information privacy regime is closely related to the European model of data protection, which provides a general right to informational privacy in a detailed regulatory regime, imposing a series of duties upon processors of personal data.

D2–1 Cybersecurity Mindset	
Awareness of cyber risks is high; there is strong private sector growth with close links to government and the military.	
D2–2 Cybersecurity Awareness	
2010 Cyber Initiative devised national education plans aimed at increasing public awareness to cyber threats.	http://sectech.tau.ac.il/cyberconference/index.php/israeli-national-cyber-bureau
D2–3 Confidence and Trust in the Internet	
E-government project "Tehila" launched in 1997 to protect the connection of government offices to internet and providing secure hosting. 81.2 percent of Israelis age 12 and over go online.	http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/Background.aspx
D2–4 Privacy Online	
Privacy is a fundamental human right under Israeli law, guaranteed by its Basic Law. It is also protected by the Privacy Protection Act of 1981.	http://www.loc.gov/law/help/online-privacy-law/israel.php

Cybersecurity Education, Training, and Skills

Dynamic

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

A central aim of the 2010 National Cyber Initiative was to devise national education plans aimed at increasing public awareness about cyber threats. Israel is rapidly accelerating its efforts to recruit and develop the cyber expertise it needs to stay ahead of the rapidly growing number of global threats. Israel invests heavily in education for the technical skills required for cybersecurity.

As part of a major national initiative to develop the south of Israel, the country is in the process of developing the Beer-Sheba area as a leading cyber R&D hub. Israel hosts R&D centers from many major high-tech multinational corporations.[18] The facility includes leaders in the cyber industry, such as EMC, Lockheed Martin, Deutsche Telekom, IBM, and JVP. It also includes leading industrial academic researchers at Ben Gurion University (BGU) and leading government agencies, such as the INCB and the national CERT, IL-CERT.[19]

Israel's strategy for cultivating the next generation of cyber talent is to integrate academia, the high-tech industry, and the military. Israel's mandatory military service for young adults creates a steady flow of individuals with cybersecurity expertise. IDF Unit 8200 is a technology incubator with a particular focus on cybersecurity. The unit finds its best talent by visiting the nation's high schools to identify high-potential candidates at an early age. They target students with superior analytical capabilities who can make quick decisions and work well in a team environment. Unit 8200's technologists work

directly with their customers to develop innovative products and learn critical startup skills. The unit's alumni founded many leading Israeli companies.

The *Magshimim* (Achievers) extracurricular program—a cooperative effort between the IDF, the Ministry of Education, and NGOs—focuses on the training and development of cyber skills at the high school level. The *Gvahim* (Heights) program aims to teach high school students the basics of cyber defense, raise the bar for cyber education in Israel, and prepare students for a matriculation exam in cybersecurity.[20] The 400 students who participate in the Heights Program face a challenging and demanding workload of 900 hours. Every day they learn programming languages, networking infrastructure, and how to deal with cyber threats.[21]

Israel's flagship institution for public-private cooperation on cybersecurity training is in Beer-Sheba, home to Ben Gurion University (BGU), in the south of the country. About 1,000 of the 20,000 students who attend BGU are computer science or IT-related majors. BGU was the first Israeli university to offer a graduate cybersecurity program several years ago.[22] Israel has numerous initiatives to bolster training and education for employees and citizens in cybersecurity. In addition to the IDF's training programs, Israel benefits from growing private investment.[23]

In March 2015, the Israeli Ministry of Education announced a partnership with Lockheed Martin to create a national cybersecurity curriculum for high school students in Israel.[24] The initiative will share best practices and partner to generate workshops and competitions. During the 2014 CyberTech conference in Beer-Sheba on the campus of BGU, IBM established its Cybersecurity Center of Excellence (CCoE). The CCoE looks at market and technology trends—including cloud, mobile, web, social media, and IT—and investigates the security exposures they create and how to mitigate them.[25]

D3–1 National Availability of Cybersecurity Education and Training

Heavy investment in education for technical skills. One of the highest technical cybersecurity skill levels per capita in the world.

D3–2 National Development of Cybersecurity Education

The MFA, IDF, and higher education develop national cyber training programs. In 2013, IDF implemented the Heights Program, a high school-level cyber defense education program for students in the 10th–12th grades.	https://www.idfblog.com/blog/2014/06/08/educating-future-cyber-warfare-next-generation-soldier/

D3–3 Training and Educational Initiatives in Public and Private Sector

Strategy is to integrate academia, the high-tech industry, and the military to create the next generation of its cyber workforce.	http://www.c4isrnet.com/story/military-tech/cyber/2014/12/12/lockheed-forms-israeli-cyber-research-group/20299707/

D3–4 Corporate Governance, Knowledge and Standards

Boards and executives have good knowledge of cyber issues and standards. However, implementation across companies at every level is incomplete.

Legal and Regulatory Frameworks

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Established

Israeli cybersecurity law has developed slowly. Israeli legal and regulatory efforts pay particular attention to cybercrime and privacy protections. The mechanism used in Israel for prosecuting violations with respect to ICT is the Computers Law of 1995. The statute rules that any change, distortion, or damage to computer software, access and permission deviation in using a computer, or presenting of false output information constitutes a crime punishable by up to five years' imprisonment.[26]

Israel amended its computer law in July 2012 to bring it in line with the Budapest Convention on Cybercrime, the first international treaty on crimes committed via the Internet.[27] A new Section 6 makes it a crime to write or distribute software to infiltrate another's computer or cause that computer to print false information, or whose purpose is to infringe on another's privacy or conduct eavesdropping even without actually causing harm or interference with the compromised system. It also tracks the Budapest Convention in requiring intent for the crimes listed in Section 6.[28]

In November 2012, Israeli police announced the creation of a 60-person unit to tackle cybercrime, to reside in the Ministry of Public Security.[29] In the civilian domain, government legislation and policy have historically focused on information security—protection of data and computerized systems.

Israel's financial regulators have recently been the most active in developing new rules. In 2014, the Central Bank published guidelines on managing risk in the cloud environment. In 2015, the Supervisor of Banks issued a circular, which ordered banks to emphasize the management of cyber-related risk and to take measures to reduce risk.[30]

D4-1 Cybersecurity Legal Frameworks	
The Computers Law of 1995 prosecutes violations of ICT. It amended the law in July 2012 to bring it in line with the Budapest Convention on Cybercrime. The Privacy Protection Act of 1981 (PPA) was one of the first privacy laws of its kind in the world.	http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403293_text
D4-2 Legal Investigation	
A 60-person unit to tackle cybercrime to reside under the Ministry of Public Security was created in November 2012 in conjunction with IL-CERT.	http://www.jpost.com/National-News/Israel-Police-to-tackle-cyber-crime-with-new-unit
D4-3 Responsible Reporting	
The INCB is responsible for reporting cyber incidents and sharing within government and the private sector.	http://sectech.tau.ac.il/cyberconference/index.php/israeli-national-cyber-bureau

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Standards, Organizations, and Technologies

Strategic

Israel's attempts to regulate cybersecurity for the private sector are predominantly restricted to technological standard-setting and government-industry cooperation. Currently, two efforts stand out: the International Organization for Standardization's (ISO) ISO 27001 and 27002 standards. Both are cybersecurity standards offering ISO/IEC voluntary certifications for complying businesses. The other one worth mentioning is the Information Security Forum's (ISF) Standard of Good Practice for Information Security (SoGP), which covers a wide range of information security frameworks to reduce business risks associated with information systems.[31]

The central recommendation of the National Cyber Initiative was to establish a national cyber bureau to be an advisory body serving the government and its head. The bureau's main activities would relate to government policy and actions in the cyber sphere, incorporating both civilian and military issues. On August 7, 2011, the Government of Israel approved the establishment of the National Cyber Bureau and determined that it would serve as a propagator of cyber policies and a coordinating body, enhance national infrastructure protection from cyber attack, and advance cyber research in the industrial sphere.

In February 2015, Israel announced the creation of a new national authority for cyber defense. The primary roles of this new body will be to:[32]

1. Manage, control, and carry out operational efforts nationwide to protect cyberspace through a systemic approach that provides complete and continuous defensive solutions to cyber-attacks.
2. Operate a national Computer Emergency Response Team (CERT).
3. Strengthen and reinforce the economy's resilience through preparatory measures and regularization.
4. Design and implement a national cyber defense doctrine.
5. Perform such duties as the Prime Minister may determine, consistent with the Authority's designated mission.

According to the proposed decision, a National Cyber Directorate would comprise the national cyber headquarters, as independent units in the Prime Minister's Office. The authority will have responsibility for achieving the authority's objectives and carrying out its mission, while the national cyber headquarters will lead nationwide policy and strategy issues on cyber competency and reinforcement of Israel's role as the global spearhead in the field of cybersecurity.[33]

IL-CERT, Israel's Computer Emergency Response Team, is the country's civilian center for addressing information security and cyber events. IL-CERT is an unaffiliated professional organization that provides an address for people and organizations in Israel and worldwide to report events concerning the Internet in Israel. IL-CERT is responsible for coordinating activities that address security events proactively, sharing information and raising public awareness on issues of information security and privacy.[34] IL-CERT carries out crisis management in Israel for cyber issues, under the umbrella of the INCB. IL-CERT investigates information security events and publishes information on how to deal with future incidents and on defense tools, and it delivers quality assessments and recommendations to the public at large.[35]

The work of strengthening national infrastructure resilience is the responsibility of the new national cybersecurity authority (NCSA), established by the Prime Minister in 2015. NCSA's key objective is to strengthen Israel's national cyber resilience by consolidating strategies and sharing relevant information with all organizations. NCSA is also responsible for the maintenance of IL-CERT and all national operational-defensive efforts.

Securing sensitive information and protecting computer infrastructures are not new challenges for Israel. The framework for Critical Infrastructure Protection (CIP) in Israel was laid out in decision B/84 of the Ministerial Committee on National Security, "Responsibility for Protecting Computerized Systems in the State of Israel," on December 11, 2002. While threats have evolved, this decision continues to serve as the basis for Israeli responses to cyber threats to critical infrastructure.[36] The response mandated by the decision includes the establishment of a steering committee to identify which institutions are critical to protect, and the establishment of a government unit to protect civilian computerized infrastructure, the Information Security Authority (RE'EM).[37] RE'EM was established by Shin Bet to comply with legal restraints on government intervention in business, since by law only civilian authorities, such as the police or the GSS, can intervene in private businesses. RE'EM oversees IT security in institutions defined as critical: it provides guidance, oversees implementation, and institutes sanctions against those that violate its directives. The institutions bear the costs of the protection required.

Israel's cybersecurity market is one of the fastest growing markets in the world. In 2014, Israeli companies sold around US$6 billion of Internet security software, equivalent to about one-tenth of the world's sales in that market. Much of that valuation is thanks to Check Point, known for its ZoneAlarm antivirus software for home computers, as well as for a range of online business security products.[38] Israel is also nurturing a number of cybersecurity startups. Last year, eight of these sold to foreign investors for a total of US$700 million.[39] In addition, cyber insurance has a small but growing market in Israel.

D5-1 Adherence to Standards	
Private sector implements ISO 27001 and 27002. Both are cybersecurity standards offering ISO/IEC voluntary certifications for complying businesses.	http://www.27000.org/iso-27001.htm
D5-2 Cybersecurity Coordinating Organizations	
INCB and the new Cyber Defense Authority are responsible for coordinating cyber policy. Command and control center is located within the C4I Corps.	https://www.idfblog.com/about-the-idf/idf-units/c4i-computers-and-communications/.
D5-3: Incident Response	
IL-CERT addresses ICT and cyber events. IL-CERT is responsible for coordinating activities in addressing security events, proactive activities before they occur and information sharing and public awareness on issues of Information Security and Privacy.	https://il-cert.org.il/

D5–4: National Infrastructure Resilience

National technology infrastructure is managed through the INCB and the Information Security Authority (RE'EM), part of the Israeli Security Agency.

http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx

D5–5 Critical National Infrastructure Protection

The framework for Critical Infrastructure Protection (CIP) in Israel was laid out in decision B/84 of the Ministerial Committee on National Security, "Responsibility for Protecting Computerized Systems in the State of Israel" on December 11, 2002.

http://sectech.tau.ac.il/sites/default/files/publications/article_3_12_-_chaire_cyberdefense.pdf

D5–6 Crisis Management

Crisis management in Israel for cyber issues is carried out specifically by IL-CERT, under the umbrella of the INCB. IL-CERT investigates information security events and publishes information to the public on how to deal with future incidents and defense tools, and it delivers quality assessments and recommendations to the public at large.

https://il-cert.org.il/

D5–7 Digital Redundancy

The agencies under the INCB have responsibility for redundant cyber systems.

D5–8 Cybersecurity Marketplace

The Israeli cybersecurity market is one of the fastest growing markets in the world. In 2014 Israeli companies sold around $6 billion of Internet security software, equivalent to about a tenth of the world's sales in that market.

Notes

1. The Security and Defense Agenda (SDA) Report, Cyber-Security: The Vexed Question of Global Rules (30 January 2012): 66–67.
2. Raska, M. 2015. "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defense Strategy." RSIS Nanyang Technological University, January 2015.
3. Tabansky, L. and I. B. Israel. 2015. *Cybersecurity in Israel*. New York, NY: Springer.
4. "National Cyber Bureau," accessed October 10, 2015, http://sectech.tau.ac.il/cyberconference/index.php/israeli-national-cyber-bureau.
5. http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/Background.aspx
6. "How Israel Balances Cybersecurity, Privacy - Al-Monitor: The Pulse of the Middle East." *Al-Monitor*, accessed October 9, 2015, http://www.al-monitor.com/pulse/originals/2015/06/israel-national-cyber-bureau-shin-beth-civil-rights-privacy.html.
7. Tabansky, L. "2013. Cyberdefense Policy of Israel: Evolving Threats and Responses." *Yuval Ne'eman Workshop for Science, Technology and Security*. January 2013. http://sectech.tau.ac.il/sites/default/files/publications/article_3_12_-_chaire_cyberdefense.pdf

8. Elban, M. and G. Siboni, "Establishing an IDF Cyber Command," *INSS Insight*. July 8, 2015. http://www.inss.org.il/index.aspx?id=4538&articleid=10007

9. Sugarman, E. 2014. "What The United States Can Learn From Israel About Cybersecurity." *Forbes.* October 2014, http://www.forbes.com/sites/elisugarman/2014/10/07/what-the-united-states-can-learn-from-israel-about-cybersecurity/

10. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Israel.pdf

11. Dror, Y. "Online Privacy in Israel." The College of Management Academic Studies, Hebrew University, May 2014. http://www.colman.ac.il/research/research_institute/Israel_project_Digital/Documents/digital_reserch_2014_eng.pdf

12. "Cyber-Boom or Cyber-Bubble?" *The Economist*, August 1, 2015, http://www.economist.com/news/business/21660112-internet-security-has-become-bigger-export-earner-arms-cyber-boom-or-cyber-bubble.

13. http://sectech.tau.ac.il/cyberconference/index.php/israeli-national-cyber-bureau

14. Tabansky and Israel, *Cybersecurity in Israel*.

15. Raska, M. "The Israeli Experience." 2015. *The Straits Times*, (June 24, 2015), http://www.straitstimes.com/opinion/the-israeli-experience.

16. "Basic Law: Human Dignity and Liberty (1992)," accessed October 9, 2015, http://www.israellawresourcecenter.org/israellaws/fulltext/basiclawhumandignity.htm.

17. Birnhack, M. and K. Niva Elkin. 2011. "Does Law Matter Online? Empirical Evidence on Privacy Law Compliance," *Michigan Telecommunications and Technology Law Review* 17(2): 337–84.

18. Tabansky and Israel, *Cybersecurity in Israel*.

19. Raska, M. "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defense Strategy." RSIS Nanyang Technological University, January 2015.

20. Tabansky and Israel, *Cybersecurity in Israel*.

21. "Educating for the Future: Cyber Warfare and the Next Generation," *IDF Blog | The Official Blog of the Israel Defense Forces*, accessed October 9, 2015, https://www.idfblog.com/blog/2014/06/08/educating-future-cyber-warfare-next-generation-soldier/.

22. "Why Israel Could Be the next Cybersecurity World Power," *ITworld*, March 9, 2015, http://www.itworld.com/article/2894051/why-israel-could-be-the-next-cybersecurity-world-power.html.

23. "Why Israel Could Be the next Cybersecurity World Power."

24. "Lockheed Martin Partners With Israel on National Cyber Curriculum," accessed October 7, 2015, http://www.israeldefense.co.il/en/content/lockheed-martin-partners-israel-national-cyber-curriculum.

25. "Why Israel Could Be the next Cybersecurity World Power."

26. Fish, J."Israel Law Blog: Israel Updates Its Computer Law to Comply with the Budapest Convention," *Israel Law Blog*, July 26, 2012, http://israellawblog.blogspot.com/2012/07/israel-updates-its-computer-law-to.html.

27. Levush, R. "Global Legal Monitor: Israel: Criminalization of Certain Activities Involving Computer Software | Global Legal Monitor | Law Library of Congress | Library of Congress," web page, (August 21, 2012), http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403293_text.

28. Fish, J. "Israel Law Blog."

29. "Israel Police to Tackle Cyber Crime with New Unit." *The Jerusalem Post | JPost.com*, accessed October 9, 2015, http://www.jpost.com/National-News/Israel-Police-to-tackle-cyber-crime-with-new-unit.

30. "Israel Supervisor of Banks Issues Cyber Defense Circular," accessed October 28, 2015, http://www.law.co.il/en/news/israeli_internet_law_update/2015/03/20/banking-supervisor-issues-cyber-defense-circular/.

31. "Towards a Cybersecurity Policy Model – Israel National Cyber Bureau (INCB) Case Study," January 7, 2015, https://publixphere.net/i/noc/page/IG_Case_Study_Towards_a_Cyber_Security_Policy_Model_Israel_National_Cyber_Bureau_INCB.

32. "Cabinet Approves Establishment of National Cyber Authority 15 Feb 2015," accessed October 28, 2015, http://mfa.gov.il/MFA/PressRoom/2015/Pages/Cabinet-approves-establishment-of-National-Cyber-Authority-15-Feb-2015.aspx.

33. "Broad Powers to a New Israeli National Cyber Defense Authority," accessed October 9, 2015. http://www.law.co.il/en/news/israeli_internet_law_update/2015/01/09/Broad-Powers-to-new-National-Cyber-Defense-Authority/.

34. "IL-CERT." *IL-CERT*, accessed October 9, 2015, https://il-cert.org.il/.

35. *Ibid*.

36. Tabansky, L. 2011. "Critical Infrastructure Protection against Cyber Threats," *Military and Strategic Affairs* 3(2). November: 72.

37. http://www.shabak.gov.il/about/units/reem/Pages/default.aspx

38. "Cyber-Boom or Cyber-Bubble?"

39. "US IPO Pricing Recap: CyberArk Software Pops 85% and Year's Second Largest IPO Trades Up." *NASDAQ.com*, accessed October 28, 2015, http://www.nasdaq.com/article/us-ipo-pricing-recap-cyberark-software-pops-85-and-years-second-largest-ipo-trades-up-cm396042.

.kr

Republic of Korea

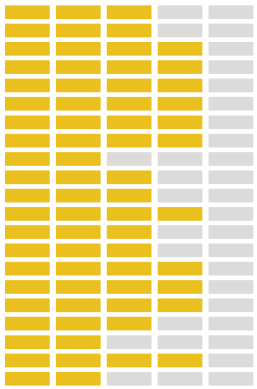
Policy and Strategy

Culture and Society

Education

Legal Frameworks

Technologies



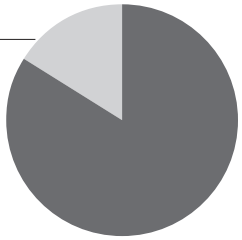
Main Cybersecurity Challenges

South Korea's cybersecurity posture reflects the challenge posed by North Korea. Cyberspace has emerged as a new arena for conflict on the Korean Peninsula. North Korea's growing cyber capabilities drive South Korean efforts to improve cybersecurity. The 2014 South Korean Defense White Paper emphasizes, "North Korea currently operates about 6,000 cyber warfare troops and conducts cyber warfare, including the interruption of military operations and attacks against major national infrastructure, to cause psychological and physical paralysis in the South."[1] According to a 2015 report, cyber attacks from North Korea have cost the country around 800 billion won (US$706 million) in economic damages.[2] Examples of North Korean cyber actions include attacks in 2013 that disrupted service at two South Korean banks and several broadcast television stations.[3] South Korean investigations of an information system breach at a nuclear plant operator in December 2014 traced back the intrusion to North Korea.[4] The attackers did not compromise critical systems managing the operation of reactors, but they did exfiltrate blueprints and test data that may be useful in planning future attacks. U.S. and South Korean defense agencies assume that in the event of a major conflict, North Korea will use cyber attacks against South Korean critical infrastructure and its command and control networks.

TOTAL POPULATION IN THE COUNTRY	**50,423,955**
Mobile cellular subscriptions	58,340,515
Internet users	42,507,394

Internet penetration

84%



Source: World Bank Development Indicators (2014). Available at http://databank.worldbank.org/data/reports.aspx?source=2&country=USA&series=&period=.

Policy and Strategy

Official National Cybersecurity Strategy

- Strategy development
- Organization
- Content

Cyber Defense Consideration

- Strategy
- Organization
- Coordination

Culture and Society

Cybersecurity Mind-Set

- Government
- Private Sector
- Society

Cybersecurity Awareness

- Awareness raising

Confidence and Trust on the Internet

- Trust in use of online services
- Trust in e-government
- Trust in e-commerce

Online Privacy

- Privacy standards
- Employee privacy

Education

National Availability of Cyber Education and Training

- Education
- Training

National Development of Cybersecurity Education

- National development of cybersecurity education

Training and Educational initiatives

- Training employees in cybersecurity

Corporate Governance, Knowledge and Standards

- Private and state-owned companies' understanding

Legal Frameworks

Cybersecurity Legal Frameworks

- Legislative frameworks for ICT security
- Privacy, data protection and other human rights
- Substantive cybercrime law
- Procedural cybercrime law

Legal investigation

- Law enforcement
- Prosecution services
- Courts

Responsible Reporting

- Responsible disclosure

Technologies

Adherence to Standards

- Implementation of Standards
- Procurement
- Software development

Cyber Security Coordinating Organizations

- Command and control center
- Incident response capacity

Incident Response

- Identification and designation
- Organization
- Coordination

National Infrastructure Resilience

- Infrastructure technology
- National resilience

Critical National Infrastructure Protection

- Identification
- Organization
- Response planning
- Coordination
- Risk management

Crisis Management

- Planning
- Evaluation

Digital Redundancy

- Planning
- Organization

Cybersecurity Marketplace

- Cybersecurity technologies
- Cybercrime insurance

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Cybersecurity Policy and Strategy

Strategic

South Korea's first cybersecurity policy was part of a larger strategy to digitize its economy. The creation in 1996 of the Korean Information Security Center—now known as the Korea Internet and Security Agency (KISA)—was one of the country's first steps in cybersecurity. Since then, its cybersecurity policies have gone through several iterations. In 2011, the Republic of Korea (ROK) announced a national cybersecurity "master plan" to respond to cyber attacks.[5] Developed jointly by 15 government agencies, the plan takes a comprehensive national approach to cybersecurity, in which cyberspace is considered another part of the nation's territory needing a national-level defense system. Under the master plan, the National Cybersecurity Center, run by the National Intelligence Service, coordinates efforts against cyber attacks among government agencies. The strategy calls for government agencies and private enterprises to encrypt and back up important data and install software to prevent cyber attacks. To oversee implementation and coordination, in March 2015, the ROK announced the appointment of a new presidential adviser dedicated to cybersecurity matters.[6]

The National Cybersecurity Master Plan rests on three pillars of investment in security capabilities, the development of a legal framework, and international cooperation. The tasks undertaken in the implementation of the document are grouped into five action plans:

1. Establishing a joint response system of private, public, and military sectors
2. Strengthening the security of critical infrastructure and enhancing secrets protection
3. Detecting and blocking cyber attacks at the national level
4. Establishing deterrence against cyber provocation and strengthening international cooperation
5. Building cybersecurity infrastructure

D1–1 National Cybersecurity Strategy

In April 2015, South Korea appointed its first cyber advisor reporting to the president within the National Security Office. This position serves as the country's 'control tower' to enable effective responses to cyber threats.	http://english1.president.go.kr/government/office-of-national-security.php

D1–2 Cyber Defense Consideration

Cyber Command was created in 2010. ROK military possesses both defensive and offensive cyber capabilities, mainly developed to counter North Korea's cyber capability.	http://m.mnd.go.kr/cop/pblictn/selectPublicationUser.do?siteId=mnd_eng&componentId=51&categoryId=0&publicationSeq=689&pageIndex=1&id=mnd_eng_021400000000

Cyber Culture and Society

Dynamic

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Korea is a world leader in IT. More than 75 percent of Koreans have mobile phones. Korea leads the United States and Europe in broadband penetration, and three-quarters of Korean households have high-speed broadband access. Two-thirds of Koreans under the age of 30 use wireless devices for Internet access. Broadband access is heavily subsidized, and the Korean government actively promotes the use of the Internet as part of a larger innovation strategy.[7]

To promote a resilient cyber culture, the ROK endeavors to raise general awareness about cybersecurity, shares best practices, and sends out specific threat alerts. In addition to the annual Information Security Awareness Month, the Korean Communications Commission in October 2013 launched the Internet Safety Keeper campaign that enlisted celebrity ambassadors to speak on TV and radio about personal data protection. Complementing this initiative were banners and ads on subways and buses, in shopping malls, and in gaming halls.[8]

As part of this public effort, KISA runs a "cyber vaccination program," collaborating with Internet service providers to identify and reach out to users whose computers have been hijacked by a botnet. Free tools to remove malware known to co-opt computers into networked attacks are also made available online. As users increasingly move toward smart mobile devices, government security solutions have extended coverage of the spectrum. The Phone Keeper app screens a user's phone for malware and stops the user from accidentally opening links from phishing texts that lead to infected websites.[9]

D2-1 Cybersecurity Mindset

South Korea is renowned as the world's most connected country, so cybersecurity and policy issues are frequently discussed in traditional media, social media, and academic debates. Digital media play an increasingly important role in informing the opinions of South Koreans.

D2-2 Cybersecurity Awareness

KISA and the Korean Communications Commission have each launched cyber awareness campaigns to promote resilience among the population.

http://isis.kisa.or.kr/eng/ebook/EngWhitePaper2014.pdf

D2-3 Confidence and Trust in the Internet

An estimated 85 percent of South Koreans are connected to the Internet, which plays a central role in commerce.

D2-4 Privacy Online

Privacy protections for online activity are weak, and the government has been criticized for attempting to control content critical of government policy.

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Cybersecurity Education, Training and Skills

Strategic

South Korea's approach to cybersecurity education and training seeks to harness its compulsory national military service program, world-class engineering and computer science universities, and its robust business sector. The South Korean military has established numerous educational and training programs to build cyber expertise. In collaboration with the Ministry of Science, ICT and Future Planning, the military created a program in 2015 to hire professional manpower directly from the private sector. Korea University has also established the Department of Cyber Defense, which plans to foster specialized cyber experts.[10] Regulations requiring large corporations to hire Chief Information Security Officers have driven an increase in demand for cyber-competent personnel.

KISA has supported the formation of partnerships between colleges and private sector companies to streamline the academic program directly to business needs and secure employment for students early on in their training. Another KISA initiative was the Academy of Knowledge Information Security, designed to address the shortfall of professionals in the disciplines of digital forensics, bio recognition, RFID/ USN security, and knowledge information security consulting.[11] High initial investment costs in these fields have led to a mismatch of limited training opportunities at existing institutions and greater demand for experts in these areas in the labor market.[12]

Since 2005, KISA, through the Asia-Pacific Information Security Training Course, has assisted developing countries in building national CERTs. Government employees receive best-practice guidance at the Informational Education Center run by the Department of Informatization Manpower Development under the Ministry of Security and Public Administration.[13]

In 2008, the Ministry of Education set up the Educational Cybersecurity Center (ECSC) to help enhance security standards at the source of intellectual property development at research universities. As of 2013, 406 institutions were participating, 308 of which have established local control centers. ECSC exchanges information and coordinates incident response with KrCERT and the National Cybersecurity Center.[14]

D3–1 National Availability of Cyber Education and Training

KISA has launched the Academy of Knowledge Information Security, and the Ministry of Information and Communication organizes IT expert training campaigns each year.	https://www.kisa.or.kr/eng/main.jsp

D3–2 National Development of Cybersecurity Education

Part of South Korea's strategy to establish an ICT knowledge base involves being a "people-powered nation." As such, information security education opportunities continue to expand.	http://www.klink.or.kr/pages/program/program.jsp

D3–3 Training and Educational Initiatives in Public and Private Sector	
South Korea's ICT sector has a close relationship with government, and public-private initiatives exist and are growing. The National Information Security Alliance (NISA) is composed of representatives of public and private sector and academic institutions.	http://itlaw.wikia.com/wiki/National_Information_Security_Alliance
D3–4 Corporate Governance, Knowledge and Standards	
A close relationship between industry and the government has encouraged the growth of e-commerce and the implementation of effective standards for cyber reporting.	http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_K1V4V0O2U2M7N0L0Z3B1T3J8X6Z0E9

Legal and Regulatory Frameworks

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Established

South Korea does not have comprehensive cybersecurity or critical infrastructure legislation. It relies on a number of laws and regulations on the protection of information, including laws on military secrets, telecommunications, cybercrime, e-government, and information infrastructure protection. The most important of these are the National Cyber Terrorism Prevention Act, the Information and Communications Infrastructure Protection Act, the Privacy Act, and the National Cybersecurity Management Regulation (Presidential Directive 141).

The first law in South Korea dedicated to cybersecurity dates to 1995, when the Framework Act on Informationalization Promotion[15] made information security a government responsibility.[16] The Act outlined the responsibilities of KISA, as well as reporting requirements for information and communication service providers. This law was followed by the 2002 Act on the Protection of Information and Communications Infrastructure and the 2003 Act on Promotion of Information and Communications Network Utilization and Information Protection, which provide the legislative basis for the enforcement of cybercrime law in South Korea.[17]

The 2006 Act on Prevention of Divulgence and Protection of Industrial Technology[18] provided for the suspension and outright ban of the export of technologies considered to undermine South Korea's national security posture. The 2009 Information and Communications Technology Industry Promotion Act, which seeks to create a domestic environment supportive of the ICT sector, includes a section on strengthening information security. The Digital Signature Act governs the distribution of public certificates.

The Electronic Government Act[19] outlines authentication procedures and the accepted certificates used to ensure security in the digital delivery of government services. Remaining privacy concerns are addressed by the Act on the Protection of Personal Information Stored and Maintained by Public Agencies.

The Act on the Development of Cloud Computing and Protection of Users, which went into effect in September 2015, is the first of its kind. Cloud service providers are obliged to report data leakages to affected users. Moreover, the Act explicitly forbids sharing personal information with any third parties and requires service providers to destroy these information records upon discontinuation of their service. The Act holds service providers accountable for damages caused to users in the event of network intrusions.[20]

D4–1 Cybersecurity Legal Frameworks	
The Criminal Act, the Act on Promotion of Information and Communications Network Utilization and Information Protection, the Personal Information Protection Act and the Act on the Protection of Information and Communications Infrastructure provide the legislative basis for enforcement of cybercrime law in South Korea.	http://www.worldlii.org/int/other/PrivLRes/2005/2.html
D4–2 Legal Investigation	
The National Police Agency's Cyber Bureau was established in June 2014, but a computer crime investigation team was first established in 1997.	www.netan.go.kr/eng/index.jsp
D4–3 Responsible Reporting	
The Korea Communications Commission (KCC) is the regulatory body responsible for reporting cyber data breach incidents. Recent data breach amendments (Bill No. 10479) to South Korea's framework data protection law increase fines, lower the liability threshold that regulators must meet to levy fines, allow compensation of individual plaintiffs without proving damages, and require notification of affected individuals within 24 hours of discovering a breach.	http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_K1V4V0O2U2M7N0L0Z3B1T3J8X6Z0E9

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Standards, Organizations, and Technologies

Strategic

Korea has a number of different organizations with cybersecurity responsibilities. The Ministry of National Defense (including the subsidiary ROK Cyber Command), the Ministry of Science, ICT and Future Planning, the National Intelligence Service, and the Ministry of Security and Public Administration are the primary bodies for cybersecurity. Threat awareness and information sharing with the private sector are the responsibility of KISA.

The National Cybersecurity Center (NCSC), part of the National Intelligence Service, is the lead agency for investigating and analyzing cybersecurity incidents in the ROK. During crises, the National Cyber Threat Joint Response Team, composed of military, civilian and private sector entities, reinforces the Center. Management of cyber incidents—public and private—falls to the Korean Computer Emergency Response Team/ Coordination Center (KnCERT/CC).

There are no specific cybersecurity standards or certification requirements for procurement in South Korea. Where general IT procurement requirements are in place, they sometimes include unique local requirements. South Korea has also introduced some local testing requirements for products that have already received international accreditation. Although South Korea participates in the Common Criteria Recognition Arrangement (CCRA), in practice a combination of unique local requirements and additional local testing acts as a barrier to the proper implementation of the CCRA.[21] The ROK has its own Korea Evaluation and Certification Scheme (KECS) to promote the use of certified and validated IT security products and systems and to enhance the security level of the national information and communications networks. These requirements are being formalized as part of all government procurement policies.[22]

D5-1 Adherence to Standards

South Korea participates in the CCRA, in practice a combination of unique local requirements, and additional local testing acts as a barrier to the proper implementation of the CCRA. The ROK has its own Korea Evaluation and Certification Scheme to promote the use of certified and validated IT security products and systems.	https://www.commoncriteriaportal.org/ccra/members/ http://www.ipa.go.jp/event/iccc2005/pdf/B1-09B.pdf

D5-2 Cybersecurity Coordinating Organizations

In April 2015, President Park appointed Brigadier General Shin In-Seop as South Korea's cybersecurity czar within the National Security Office. This position is designed to further strengthen the country's 'control tower' and enable more effective responses to cyber threats.	http://english1.president.go.kr/government/office-of-national-security.php

D5-3: Incident Response

South Korea maintains an effective CERT capacity. KrCERT, under KISA, works with the private sector, while KnCERT is responsible for public-sector responses as a part of the National Cybersecurity Center, and for engagement with private CERTs.	http://eng.krcert.or.kr/main/main.jsp

D5-4: National Infrastructure Resilience

This issue has not been explicitly addressed.

D5-5: Critical National Infrastructure (CNI) Protection

Korea's PM office, National Cybersecurity Center (NCSC), and Ministry of Science and ICT Future protect CNI.	https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/presentations/dr-so-jeong-kim-national-security-research-institute-s-korea-cyber-security-in-the-republic-of-south-korea

D5-6: Crisis Management

KnCERT and KrCERT are responsible for cyber crisis management.	http://service1.nis.go.kr

D5-7: Digital Redundancy

This issue has not been explicitly addressed.

D5-8: Cybersecurity marketplace

South Korea's business community has a close relationship with the government, which supports businesses' efforts to grow. This has extended to the digital economy, in which government funding supports a strong startup sector.

Notes

1. Ministry of the Defense of the Republic of Korea. 2015. *2014 Defense White Paper*. http://m.mnd.go.kr/cop/pblictn/selectPublicationUser.do?siteId=mnd_eng&componentId=51&categoryId=0&publicationSeq=689&pageIndex=1&id=mnd_eng_021400000000.
2. "Cybercrime in Asia: A Changing Regulatory Environment. Marsh Asia," accessed October 23, 2015, http://asia.marsh.com/NewsInsights/ID/41587/Cybercrime-in-Asia-A-Changing-Regulatory-Environment.aspx.
3. Cluley, F. 2013. "DarkSeoul: SophosLabs Identifies Malware Used in South Korean Internet Attack, " nakedsecurity.sophos.com, March 20, 2013, https://nakedsecurity.sophos.com/2013/03/20/south-korea-cyber-attack/; "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War," Symantec Official Blog, June 26, 2013, http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war.
4. Park, J.-M. and M. Cho. 2015. "South Korea Blames North Korea for December Hack on Nuclear Operator," March 17, 2015, http://www.reuters.com/article/2015/03/17/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317.
5. https://ccdcoe.org/sites/default/files/strategy/KOR_NCSS_2011.pdf.
6. "South Korea Beefs Up Cybersecurity With an Eye on North Korea." *The Diplomat*, accessed October 22, 2015, http://thediplomat.com/2015/04/south-korea-beefs-up-cyber-security-with-an-eye-on-north-korea/.
7. "Why Internet Connections Are Fastest in South Korea - CNN.com," accessed October 27, 2015, http://edition.cnn.com/2010/TECH/03/31/broadband.south.korea/.
8. Ministry of Science, ICT and Future Planning of the Republic of Korea and Korea Internet and Security Agency. 2014. *Korea Internet White Paper,* 93-4, http://isis.kisa.or.kr/eng/ebook/EngWhitePaper2014.pdf.
9. "South Korean Schools Are Remotely Disabling Students' Smartphones." *The Verge*, accessed October 27, 2015, http://www.theverge.com/2014/3/20/5528842/korean-schools-block-smartphones-in-class-ismartkeeper.

10. Korea Development Institute and Ministry of Strategy and Finance of the Republic of Korea. 2011. "Eight Key Areas of ICT Development in Korea and Three High Priority Initiatives in Abu Dhabi's ICT Development." May 2011, 276, http://cid.kdi.re.kr/cid_eng/public/report_read05.jsp?1=1&pub_no=12035

11. The acronym stands for radio-frequency identification/ ubiquitous sensor network.

12. *Eight Key Areas of ICT Development in Korea*, 279.

13. *Ibid.,* 267.

14. *2013 White Paper on ICT in Education Korea*, 106.

15. Renamed the Framework Act on National Informatization in 2009.

16. A complete overview of Internet-related laws currently in force (as of June 2014) is available in the 2014 Korea Internet White Paper, 95.

17. The Act on Promotion of Utilization of Information and Communications Network had been renamed Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

18. Act on Prevention of Divulgence and Protection of Industrial Technology, Republic of Korea, Act No. 8062 of October 27, 2006, as last amended by Act No. 11690 on March 23, 2013, http://www.wipo.int/wipolex/en/details.jsp?id=13745.

19. Electronic Government Act, Republic of Korea, Act No. 8171 of January 3, 2007, as last amended by Act No. 11461 on June 1, 2012, http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=25509&type=new&key.

20. Galeote, R. 2015. "South Korea: National Assembly Passes 'World-first' Cloud Computing Act," DataGuidance.com, March 19, 2015, http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=3459.

21. "Members of the CCRA : New CC Portal," accessed October 23, 2015, http://www.commoncriteriaportal.org/ccra/members/.

22. "Welcome to ITSCC," accessed October 23, 2015, http://www.itscc.kr/eng/main.asp.

.us

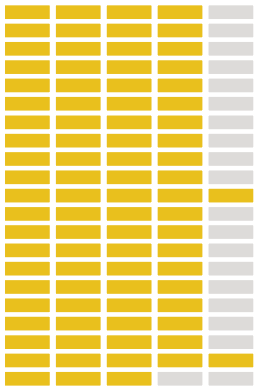
Policy and Strategy

Culture and Society

Education

Legal Frameworks

Technologies



United States of America

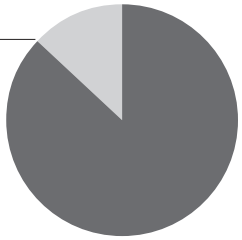
Main Cybersecurity Challenges

The United States has a complex and evolving set of rules, institutions, and policies to manage the challenge of cybersecurity. These efforts began almost 20 years ago in the 1990s, but it has only been in the last six years that an integrated and compressive approach has emerged. U.S. authorities regard cyber threats as the leading strategic threat to the United States.[1] The United States has experienced a sustained campaign of economic espionage and financial crime from the Internet and faces the risk of attacks on critical infrastructure and services. Losses to the American economy reach billions of U.S. dollars every year. The last year has been particularly difficult, with coercive attacks against Sony Pictures, the Sands Casino, and Github, a hosting service. The United States has detected that a number of countries have probed its critical infrastructure looking for vulnerabilities for use in a cyber attack.

TOTAL POPULATION IN THE COUNTRY	**318,857,056**
Mobile cellular subscriptions	351,380,475
Internet users	278,681,066

Internet penetration

87%



Source: World Bank Development Indicators (2014). Available at http://databank.worldbank.org/data/reports.aspx?source=2&country=USA&series=&period=.

Policy and Strategy

Official National Cybersecurity Strategy

- Strategy development
- Organization
- Content

Cyber Defense Consideration

- Strategy
- Organization
- Coordination

Culture and Society

Cybersecurity Mind-Set

- Government
- Private Sector
- Society

Cybersecurity Awareness

- Awareness raising

Confidence and Trust on the Internet

- Trust in use of online services
- Trust in e-government
- Trust in e-commerce

Online Privacy

- Privacy standards
- Employee privacy

Education

National Availability of Cyber Education and Training

- Education
- Training

National Development of Cybersecurity Education

- National development of cybersecurity education

Training and Educational initiatives

- Training employees in cybersecurity

Corporate Governance, Knowledge and Standards

- Private and state-owned companies' understanding

Legal Frameworks

Cybersecurity Legal Frameworks

- Legislative frameworks for ICT security
- Privacy, data protection and other human rights
- Substantive cybercrime law
- Procedural cybercrime law

Legal investigation

- Law enforcement
- Prosecution services
- Courts

Responsible Reporting

- Responsible disclosure

Technologies

Adherence to Standards

- Implementation of Standards
- Procurement
- Software development

Cyber Security Coordinating Organizations

- Command and control center
- Incident response capacity

Incident Response

- Identification and designation
- Organization
- Coordination

National Infrastructure Resilience

- Infrastructure technology
- National resilience

Critical National Infrastructure Protection

- Identification
- Organization
- Response planning
- Coordination
- Risk management

Crisis Management

- Planning
- Evaluation

Digital Redundancy

- Planning
- Organization

Cybersecurity Marketplace

- Cybersecurity technologies
- Cybercrime insurance

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Cybersecurity Policy and Strategy

Strategic

A 1998 White House Commission on Critical Infrastructure Protection predicted that the increasing U.S. reliance on cyber-based information systems would create "a new dimension of vulnerability."[2] The report determined that cyber attacks on infrastructure and information systems could significantly harm the U.S. economy and security.

In response, the White House created the Presidential Decision Directive 63 (PDD-63), which directed agencies to take necessary steps to ensure the continuity and viability of critical infrastructure. PDD-63 established a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism (a senior White House staff member). PDD-63 created public-private partnerships. The president designated lead agencies in the federal government for specific critical infrastructure sectors. Although PDD-63 called for the creation of a single Information Sharing and Analysis Center (ISAC), individual critical infrastructure sectors established their own, sector-specific ISACs. Their effectiveness varies across sectors with some, such as the Financial Services ISAC, standing out as successes. The Multi-State Information Sharing and Analysis Center provides information to local and state governments in all 50 states, U.S. territories, and districts.[3] These steps proved to be insufficient, leading the White House to produce the 2008 Comprehensive National Cybersecurity Initiative (CNCI).[4] The elements of the CNCI included:[5]

- Managing government networks as a single enterprise using the "Trusted Internet Connections" program.
- Deploying intrusion detection and intrusion prevention systems across the government.
- Coordinating R&D efforts.
- Connecting federal cyber operations centers.
- Developing and implementing a government-wide cyber counterintelligence plan.
- Increasing the security of classified networks.
- Expanding cyber education.
- Developing deterrence strategies and programs.
- Managing supply chain risk.
- Defining the federal role for cybersecurity in critical infrastructure.

Only a few of these initiatives were successful. Shortly after taking office in 2009, President Obama ordered a review of federal efforts such as the CNCI and asked the National Security Council to develop a comprehensive approach to cybersecurity. The resulting Cyberspace Policy Review recommended a number of steps:[6]

- Create a Cybersecurity Coordinator;
- Work with state and local governments and the private sector to ensure a unified response to future cyber incidents;

- Strengthen public-private partnerships;
- Invest in cutting-edge research and development; and
- Begin a campaign to promote cybersecurity awareness and build the digital workforce.

In 2011, the Obama administration also developed an International Strategy for Cyberspace, emphasizing "stability through norms" and created the position of Cybersecurity Coordinator at the Department of State.[7]

D1-1 National Cybersecurity Strategy	
The Comprehensive National Cybersecurity Initiative of 2008 and the 2009 Cyberspace Policy Review outline the U.S. cyber strategy.	https://www.whitehouse.gov/node/233086 https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
D1-2 Cyber Defense Consideration	
Strategy is outlined in the 2015 Department of Defense Cyber Strategy.	http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Cyber Culture and Society

Dynamic

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

The United States has one of the most vibrant cyber cultures in the world. In the last few years, a series of high-profile breaches has brought cybersecurity to the forefront of public awareness. A number of separate initiatives facilitate cybersecurity awareness. The Federal Trade Commission (FTC) provides briefs on data security for businesses.[8] The National Cyber Awareness System, part of the U.S. Computer Emergency Readiness Team, monitors the threat environment, issuing timely alerts about exploitation trends.[9] An aggregate government-maintained repository of known vulnerabilities exists in the National Vulnerability Database (NVD).[10] The Security Content Automation Protocol created under the National Institute of Standards and Technology (NIST) operationalizes the information gathered in NVD, setting the configurations of operating systems and applications to safe standards.

The annual National Cybersecurity Awareness Month, created by the National Cybersecurity Alliance, a private sector group, and the Department of Homeland Security (DHS) in 2004, promotes a culture of cybersecurity at work and the safe use of Internet-connected devices. It aims to inspire students to pursue a career in cybersecurity.[11] It launched the *Stop.Think. Connect*. campaign[12] to create an understanding of cybersecurity requirements.

D2–1 Cybersecurity Mindset

The United States has one of the most vibrant cyber cultures in the world. In the last few years, a series of high-profile breaches has brought cybersecurity to the forefront of public awareness.

D2–2 Cybersecurity Awareness

The National Cyber Awareness System set up with the U.S. CERT monitors the threat environment, issuing timely alerts about exploitation trends.

https://www.us-cert.gov/ncas

The FTC provides briefs on data security for businesses.

https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf

D2–3 Confidence and Trust in the Internet

Confidence and trust in the Internet are high, despite numerous high-profile breaches of corporate and personal data in recent years.

D2–4 Privacy Online

There is no overarching online privacy law in the United States; however, individual states have passed laws to protect individual Internet users.

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Cybersecurity Education, Training, and Skills

Strategic

The United States is home to strong university programs on both the technical and policy sides of the cybersecurity spectrum. The Department of Education and the National Science Foundation (NSF) collaborate in training the next generation of cybersecurity professionals. The cybersecurity component of the Advanced Technological Education (ATE) programs[13] offered by the NSF prepares technicians. ATE centers further share their expertise and resources to facilitate cybersecurity programs at community colleges.[14]

The National Security Agency (NSA) and DHS have built a network of National Centers for Academic Excellence in the areas of cyber defense[15] and cyber operations,[16] with universities nationwide participating. Under the auspices of the National Initiative for Cybersecurity Education (NICE), these programs work to close the cybersecurity skill gap—expanding the scope and improving the standard of education efforts—and provide early assistance in career development to attract a larger pool of talent to the discipline.[17] Increasing the share of underrepresented populations to enhance diversity is a stated goal of the initiative. NICE has created a series of scholarships dedicated to cybersecurity.[18]

NICE provides analytical tools to help businesses and agencies in their workforce planning[19] by assessing their human capital requirements based on the institution's capability, maturity, and skill deficits.[20] The education and training catalog hosted by the National Initiative for Cybersecurity Careers and Studies (NICCS) assists employees in their professional development, with currently over 1,300 courses offered.[21]

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) offers regular training opportunities through its virtual learning portal specifically targeted at ICS security personnel.[22]

Most decisions about the content and structure of curricula in the United States are made by private educational institutions or determined at the state level. Thus, the effect of federal policy is limited. Providing an informal framework through national cyber competitions[23] and free instructional material has since been the federal strategy for elevating the position of cybersecurity within existing educational programs. The Cybersecurity Education and Awareness branch of DHS has developed STEM-oriented curricula for middle- and high-school teachers that integrate aspects of cybersecurity.[24] The Cybersecurity Education and Training Assistance Program support these.[25]

D3-1 National Availability of Cyber Education and Training

The NSA and DHS have built a network of National Centers for Academic Excellence in the areas of cyber defense and cyber operations with universities nationwide. Under the auspices of the NICE, these programs work to close the cybersecurity skill gap.	http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

D3-2 National Development of Cybersecurity Education

The NICE addresses cybersecurity education and workforce development. Locally, there have been efforts to make cybersecurity part of standard curricula, but no federal guidance exists.	http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

D3-3 Training and Educational Initiatives in Public and Private Sector

NICE provides analytical tools to help businesses and agencies by assessing their human capital requirements. The education and training catalog hosted by the National Initiative for Cybersecurity Careers and Studies assists employees generally in their professional development with currently over 1,300 courses registered. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) through its virtual learning portal offers regular training opportunities specifically targeted at ICS security personnel.	https://niccs.us-cert.gov/education/scholarship-opportunities

D3-4 Corporate Governance, Knowledge and Standards

Awareness of cybersecurity issues among U.S. companies at the highest levels, after several high-profile corporate breaches in recent years. Adherence to standards is strong in the financial sector and improving elsewhere.	http://www.ponemon.org/library/2014-a-year-of-mega-breaches

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Legal and Regulatory Frameworks

Dynamic

The United States has no overarching cybersecurity law and relies on a variety of regulatory regimes and legal frameworks. Most of these are sector-specific. The financial industry has been among the most active sectors in this area, with guidance issued in recent years by the Office of the Comptroller of the Currency, the Securities and Exchange Commission (SEC), the Federal Financial Institutions Examination Council, the Federal Reserve, and the Financial Regulation Authority.[26] In 2006, the Federal Reserve released "Operating Circular No. 5: Electronic Access," which outlined cybersecurity requirements for firms connecting to Federal Reserve payment systems.[27]

Of the binding regulations, the Bank Secrecy Act of 1970 required firms to implement IT management systems to prevent illicit transactions and to notify the Financial Crime Enforcement Network of any known or suspicious activities.[28] The Gramm-Leach-Bliley Act of 1999 (GLBA) created personal data security requirements for the financial sector. The "Safeguards Rule" under GLBA requires financial firms to establish a written information security plan to protect and prevent unauthorized disclosure of consumers' personal data.[29] In 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which focused on information security standards to prevent identity theft by requiring disposal of information in consumer reports and records beginning in June 2005.[30]

The Energy Policy Act of 2005 gave the Federal Energy Regulatory Commission (FERC) authority to oversee the reliability of the bulk power system.[31] This includes authority to approve mandatory cybersecurity reliability standards. The North American Electric Reliability Corporation (NERC), certified by FERC as the nation's electric reliability organization, developed Critical Infrastructure Protection (CIP) standards, which were approved in January 2008.[32] In developing smart-grid technology across the United States, the Energy Independence and Security Act of 2007 (EISA) gave FERC and NIST responsibilities related to coordinating the development of guidelines and standards.[33]

The FTC has authorities to police anti-competitive practices related to data security and privacy. The FTC has brought legal action against organizations that have violated consumers' privacy rights or misled them by failing to safeguard sensitive consumer information. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition, the agency also enforces other federal laws relating to consumers' privacy and security.[34]

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. HIPAA defines policies, procedures, and guidelines for maintaining the privacy and security of personally identifiable health information, as well as outlining numerous offenses relating to health care and sets civil and criminal penalties for violations.[35]

The primary federal anti-hacking statute is the Computer Fraud and Abuse Act (CFAA) of 1986. This law makes it a crime to intentionally access a computer "without authorization" or "in excess of authorization."[36] The Economic Espionage Act of 1996 makes the theft or misappropriation of a trade secret a crime. There are also numerous other federal cybercrime laws involving Internet fraud, including mail and wire fraud, credit card fraud, and money laundering; online child pornography; the Internet sale of controlled drugs or other substances, firearms, alcohol, and gambling; as well as

software piracy and intellectual property theft. These laws have been reinforced by Executive orders for CIP, information sharing,[37] and cyber sanctions.[38] In February 2013, President Obama signed Executive Order 13636, Improving Critical Infrastructure Cybersecurity, to raise the level of core capabilities for managing cyber risk to the critical infrastructure sector. The order focused on information sharing, privacy, and the adoption of cybersecurity practices.[39] It also tasked NIST to work with the private sector to identify existing voluntary consensus standards and industry best practices and build them into a Cybersecurity Framework, which was released in February 2014.[40]

Forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information. Most U.S. states have enacted such laws since 2002 in response to an escalating number of breaches of consumer databases containing personally identifiable information. The first such law, the California Data Security Breach Notification Law, was enacted in 2002.[41] In general, most state laws follow the basic tenets of California's original law: companies must immediately disclose a data breach to customers, usually in writing. California has since broadened its law to include compromised medical and health insurance information.[42]

The SEC issued guidance in October 2011 on disclosure obligations relating to cybersecurity risks and cyber incidents. The guidance states that even though no rules explicitly address this topic, cyber incidents and the risk of such incidents may nevertheless give rise to disclosure obligations under current SEC rules, particularly the existing obligation to disclose information that a "reasonable investor would consider important to an investment decision" contained within the Securities Act of 1933 and the Securities Exchange Act of 1934.[43]

D4-1 Cybersecurity Legal Frameworks	
The United States has no overarching cybersecurity law and relies on a variety of regulatory regimes and legal frameworks. Most are sector-specific. Cybercrime is prosecuted under the Computer Fraud and Abuse Act (CFAA) of 1986. Various other laws and executive orders govern this capacity as well.	https://www.fas.org/sgp/crs/natsec/R42114.pdf
D4-2 Legal Investigation	
Multiple agencies in the United States are responsible for legal investigation of cybercrime, led by the Department of Justice (DoJ).	http://www.justice.gov/usao/priority-areas/cyber-crime
D4-3 Responsible Reporting	
The SEC issued guidance in October 2011 on disclosure obligations relating to cybersecurity risks and cyber incidents. To date, 47 states have enacted legislation requiring private or government entities to notify individuals of security breaches involving personally identifiable information.	http://csis.org/publication/evolution-cybersecurity-requirements-us-financial-industry

STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC

Standards, Organizations, and Technologies

Strategic

Responsibility for cybersecurity is shared among many agencies, each with its own set of responsibilities and authorities. The most important are the DHS, the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI), and the Departments of State and Defense. DHS is the lead agency domestic cybersecurity, and its National Protection and Programs Directorate (NPPD) has operational responsibility. NPPD is hampered by a lack of both resources and legislative authority. NPPD houses the National Cybersecurity and Communications Integration Center (NCCIC), which includes both US-CERT and ICS-CERT.[44] US-CERT develops detection and prevention mechanisms for federal institutions. It also provides information about the threat environment to private sector organizations and international partners. ICS-CERT operates through public-private partnerships with critical infrastructure companies, offering monitoring, analytic services, and response assistance to critical infrastructure and key resource organizations.

The FBI is the lead agency for the investigation of cybercrime (the Secret Service, which falls under DHS, also investigates financial cybercrime). Both the FBI and the National Security Agency (part of DOD) support DHS in its domestic cybersecurity mission. In recent years the Departments of the Treasury, Commerce, and Energy have also played active roles. The FTC and the Federal Communications Commission, two independent agencies, play a significant role in policymaking. The White House Cybersecurity Coordinator—a position created after the 2009 Cyberspace Policy Review—leads the interagency development of national cybersecurity strategy and policy, and oversees agencies' implementation of those policies.[45] The most important development is the creation of the NIST Cybersecurity Framework. This framework was created through a long process of consultation with the private sector and assembles best practices for network security. The president tasked sector-specific regulatory agencies to ensure that their existing regulations implement the cybersecurity goals of the NIST Framework. For example, the Department of Energy launched a Cybersecurity Capability Maturity Model (C2M2) program. C2M2 services are available to organizations of any size, to assess how well they are implementing the NIST Framework.[46] The financial sector has adopted key elements of standards frameworks, including those of NIST in the 2013 Cybersecurity Framework, as well as standards from the ISO and the Information Systems Audit and Control Association (ISACA).

The United States is a leader in information and cybersecurity technology. Cybersecurity has become an investment priority for both the government and the private sector. Last year, venture capitalists invested over US$1 billion in cybersecurity startups. Seventeen venture capital firms in Silicon Valley focus on developing innovative cybersecurity technologies. Last year, these Silicon Valley venture capital firms invested in more than 230 cybersecurity startups. The Defense Advanced Research Projects Agency and the National Science Foundation have also made significant investments in cybersecurity R&D.

D5-1 Adherence to Standards

The creation of the NIST Framework has added impetus to the use of cybersecurity standards.	http://www.nist.gov/cyberframework/

D5-2 Cybersecurity Coordinating Organizations

The White House Cybersecurity Coordinator—a position created after the 2009 Cyberspace Policy Review—leads the interagency development of national cybersecurity strategy and policy, and oversees agencies' implementation of those policies.	http://www.dhs.gov/national-cybersecurity-communications-integration-center https://www.whitehouse.gov/blog/author/michael-daniel

D5-3: Incident Response

The National Cybersecurity and Communications Integration Center (NCCIC)—a division within DHS—houses both US-CERT and ICS-CERT.	https://www.us-cert.gov/

D5-4: National Infrastructure Resilience

US-CERT completes the Cyber Resilience Review (CRR).	https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf
The 2015 Sector-Specific Plans supplement the National Infrastructure Protection Plan (NIPP) at DHS.	http://www.dhs.gov/critical-infrastructure-security-resilience-month

D5-5 Critical National Infrastructure Protection

The National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.	http://www.dhs.gov/national-infrastructure-protection-plan

D5-6 Crisis Management

The U.S. military cyber commands and the U.S. Computer Emergency Readiness Team (US-CERT) are responsible for cyber crises in the military and CNI/private sector, respectively.	https://www.us-cert.gov/

D5-7 Digital Redundancy

US-CERT addresses issues of digital redundancy and resilience.	https://www.us-cert.gov/

D5-8 Cybersecurity Marketplace

The United States has a large and growing cybersecurity technologies market. Cyber insurance is also gaining popularity in possibly protecting U.S. companies financially in case of incident.	

Notes

1. "Special Report: Cyber Strategy," accessed October 13, 2015, http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
2. http://fas.org/irp/offdocs/pdd/pdd-63.htm
3. Cybersecurity Awareness Month and Toolkits, Multi-State Information Sharing & Analysis Center, accessed October 9, 2015, http://msisac.cisecurity.org/resources/toolkit/.
4. "The Comprehensive National Cybersecurity Initiative." *The White House*, accessed October 13, 2015, https://www.whitehouse.gov/node/233086.
5. *Ibid*.
6. "Cyberspace Policy Review." *The White House*, accessed October 11, 2015, https://www.whitehouse.gov/node/848.
7. "Launching the U.S. International Strategy for Cyberspace." *Whitehouse.gov*, accessed October 13, 2015, https://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace.
8. Data Security, U.S. Federal Trade Commission, accessed October 9, 2015, https://www.ftc.gov/datasecurity.
9. National Cyber Awareness System, US-CERT, accessed October 9, 2015, http://www.us-cert.gov/ncas.
10. National Vulnerability Database, NIST, accessed October 9, 2015, https://nvd.nist.gov/.
11. National cybersecurity Awareness Month 2015, U.S. Department of Homeland Security, October 14, 2015, http://www.dhs.gov/national-cyber-security-awareness-month.
12. Stop. Think. Connect. Campaign, accessed October 9, 2015, http://www.stopthinkconnect.org/.
13. Advanced Technological Education Program in Security Technologies, accessed on October 9, 2015, http://www.atecenters.org/security-technologies/.
14. O'Brien, M. and A. Kellan. 2013. "Community College Cybersecurity Program Trains 21st Century Workforce." Washington, DC: National Science Foundation. January 28. http://www.nsf.gov/news/special_reports/science_nation/cybersecurity.jsp?WT.mc_id=USNSF_51.
15. National Centers of Academic Excellence - Cyber Defense, National Security Agency, July 6, 2015, https://www.nsa.gov/academia/ncae-cd/index.shtml.
16. National Centers of Academic Excellence - Cyber Operations, National Security Agency, September 9, 2015, https://www.nsa.gov/academia/nat_cae_cyber_ops/index.shtml.
17. See "Draft Strategic Goals," National Initiative for Cybersecurity Education (NICE), September 8, 2015, http://csrc.nist.gov/nice/index.htm; The original set of goals can be found in National Initiative for Cybersecurity Education - Strategic Plan, NICE, September 2012, http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf
18. Scholarship Opportunities, National Initiative for Cybersecurity Careers and Studies (NICCS), accessed October 9, 2015, https://niccs.us-cert.gov/education/scholarship-opportunities.
19. NICE, "Best Practices for Planning a Cybersecurity Workforce," White Paper, October 3, 2012, https://niccs.us-cert.gov/sites/default/files/publications/documents/Best%20Practices%20for%20Planning%20a%20Cybersecurity%20Workforce_05312012_v4.1_DRAFT_NICE%20branded.pdf.
20. NICE, "Cybersecurity Capability Maturity Model," White Paper, July 1, 2013, https://niccs.us-cert.gov/sites/default/files/documents/files/NICE%20Capability%20Maturity%20Model%20white%20paper_06282013_FINAL_NICE%20branded_0.pdf.
21. Introduction to the Education and Training Catalog, NICCS, accessed October 9, 2015, https://niccs.us-cert.gov/training/tc/search.
22. Virtual Learning Portal, ICS-CERT, accessed October 9, 2015, https://ics-cert-training.inl.gov/lms/.
23. Cyber Competitions, NICCS, accessed October 9, 2015, https://niccs.us-cert.gov/training/tc/search/cmp/new.
24. Professional Development for Teachers, NICCS, accessed October 9, 2015, https://niccs.us-cert.gov/education/professional-development-teachers.
25. Cybersecurity Education and Training Assistance Program, program no. 97.127, Catalog of Federal Domestic Assistance, 2011, https://www.cfda.gov/index?s=program&mode=form&tab=core&id=05063b31ef34183c6e0946f51562b0c9.
26. "The Evolution of Cybersecurity Requirements for the U.S. Financial Industry | Center for Strategic and International Studies."10,16]]}}}},"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}
27. Ibid.10,16]]}}}},"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}
28. "BSA/AML Examinations," December 29, 2010, http://www.occ.gov/topics/compliance-bsa/bsa/aml-examinations/index-aml-examinations.html.
29. "Standards for Safeguarding Customer Information (Safeguards Rule) | Federal Trade Commission," accessed October 16, 2015, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/standards-safeguarding-customer.
30. "FACTA Disposal Rule Goes into Effect June 1 | Federal Trade Commission," accessed October 16, 2015, https://www.ftc.gov/news-events/press-releases/2005/06/facta-disposal-rule-goes-effect-june-1.
31. "FERC: Electric Reliability: Cyber & Grid Security," accessed October 16, 2015, http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp.
32. "Critical Infrastructure Protection Committee (CIPC)," accessed October 16, 2015, http://www.nerc.com/comm/cipc/pages/default.aspx.

33. NIST US Department of Commerce, "NIST Identifies Five," accessed October 16, 2015, http://www.nist.gov/public_affairs/releases/smartgrid_100710.cfm.

34. "2014 Privacy and Data Security Update," Federal Trade Commission, accessed October 13, 2015, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf

35. "HHS.gov," Text, *HHS.gov*, accessed October 15, 2015, http://www.hhs.gov/.

36. "18 U.S. Code Chapter 37 - ESPIONAGE AND CENSORSHIP | US Law | LII / Legal Information Institute," accessed October 15, 2015, https://www.law.cornell.edu/uscode/text/18/part-I/chapter-37.

37. "2015 Executive Orders Signed by Barack Obama," accessed October 29, 2015, https://www.archives.gov/federal-register/executive-orders/2015.html.

38. "Issuance of an Executive Order Related to Significant Malicious Cyber-Enabled Activities," accessed October 15, 2015, http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150401.aspx.

39. "Foreign Policy cybersecurity Executive Order 13636," *The White House*, accessed October 16, 2015, https://www.whitehouse.gov/node/298406.

40. "Launch of the Cybersecurity Framework | The White House," accessed July 28, 2014, http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework.

41. "Security Breach Notification Laws," accessed October 13, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

42. "California Expands Breach Notification Law to Cover Online Accounts | HL Chronicle of Data Protection," accessed October 15, 2015, http://www.hldataprotection.com/2013/11/articles/cybersecurity-data-breaches/california-expands-breach-notification-law-to-cover-online-accounts/.

43. "SEC Issues New Guidance on Disclosing Cybersecurity Risks and Incidents | WilmerHale," accessed October 16, 2015, https://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=95112.

44. National Cybersecurity & Communications Integration Center, U.S. Department of Homeland Security, accessed September 19, 2014, http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

45. "Michael Daniel," *Whitehouse.gov*, accessed October 16, 2015, https://www.whitehouse.gov/blog/author/michael-daniel.

46. Cybersecurity Capability Maturity Model Program, U.S. Department of Energy, accessed October 9, 2015, http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program.

Conclusions

From the experience of these nations, we can draw some general conclusions about what an adequate national response to the challenges of cybersecurity should look like and what best practices are available for consideration. Cybersecurity requires creating strategies, rules, and institutions to make cyberspace more stable and secure in ways that enable economic growth and maximize the benefits of information technology.

The first and foundational best practice for cybersecurity is the development of a national strategy. These strategies provide a policy framework under which countries can organize their cybersecurity efforts. The process of developing a strategy can also provide a mechanism for broad, cross-governmental coordination. In three cases, countries are already on a second iteration of these strategy or guidance documents. For each of the countries examined, strategies addressed the steps needed to make cyberspace a stable and secure platform for economic activity and reduce risk to public safety and national security. As with other areas of cybersecurity, an immediate goal of a strategy is to raise the discussion and decision making from the technical to the political level. The process of developing a national strategy can usefully contribute to this.

The second best practice is the creation of an explicit organizational structure that assigns responsibilities among ministries and offices for the various aspects of cybersecurity. The most basic organizational steps, such as improving law enforcement capabilities or creating a computer emergency response team (CERT), are a good start, but by no means adequate. Countries with more advanced cybersecurity programs have created new organizations to carry out this responsibility. In each of the four countries examined, there are varying degrees of redundancy and overlapping responsibilities, but this is perhaps unavoidable and preferable to an inadequate institutional structure.

One important aspect of this organizational best practice is the creation of some kind of central coordinating authority. Cybersecurity is the responsibility of many agencies and at times can create overlapping requirements. Each of the countries studied created new, high-level entities in the Offices of the President or the Prime Minister to oversee cybersecurity. As cybersecurity efforts matured and broadened in scope, all four countries eventually created a central coordinating body. In each case, these coordinating bodies are linked to the national security decision-making apparatus rather than to economic or law-enforcement agencies. Although none of these is at a ministerial level, their connection to the chief executive confers stature and influence.

Another best practice is the development of an adequate legal framework, based on precedents drawn from international agreements and other countries' national laws. Adequate laws for cybercrime, critical infrastructure, and data protection are crucial for cybersecurity. While each country takes a different approach to working with the private sector, reflecting different national laws and political cultures, collaborative national efforts to increase awareness in the financial and business community are a central element of each nation's practices, as are efforts to increase public awareness of how to manage cybersecurity risks.

Legal and regulatory frameworks show the greatest divergence among countries. Most rely on a patchwork of existing law and new authorities to deal with cybersecurity. Given the disparate applications of cybersecurity in so many different sectors of the economy, with different requirements and functions, this patchwork approach may make the most sense, rather than trying to write one overarching law. One area of commonality is that most of the countries found it necessary to expand legal authority to deal with cybercrime.

Each country paid particular attention to a few critical infrastructure sectors—usually finance, electric power, and government services. This choice was not the result of an explicit process of prioritization; rather, key infrastructures rely on good cybersecurity.

All of the countries examined struggle with workforce issues. There is a global shortage of workers with skills in cybersecurity, and all four countries have programs to expand their cyber workforce, usually undertaken with universities and the private sector. Israel's tech-heavy military and national conscription gave it an advantage in developing this workforce. All of the countries found it necessary to create special cybersecurity curricula and programs rather than rely on traditional computer science courses.

Three of the countries—the United States, Israel, and South Korea—have vibrant, competitive IT sectors producing goods and services for the global market. This reflects conscious decisions (made decades ago in the case of the United States) to support the IT sector with investment and incentives. Importantly, Israeli and U.S. companies are not national champions directly subsidized by the government. This introduces entrepreneurial and innovative aspects to company behavior. Companies move in the direction of the market, supported by the government, rather than the other way around.

International cooperation, confidence building, sharing of best practices and information, and laying the groundwork for a stable cyber environment are also common elements in the practices of all four countries. This cooperation can range from CERT-to-CERT to high-level diplomatic activities, but it is essential and it provides countries with access to external information and technical resources. The four countries each drew on alliances to strengthen their cyber defenses, and Estonia, the smallest, was the most active internationally.

These brief assessments are a description of how leading countries have approached the problem of cybersecurity and how their approaches have evolved. All share a goal of managing cyber risk to make cyberspace no riskier than any other activity. How each country approaches this challenge will be shaped by its history, culture, and institutions. In all four countries studied, cybersecurity is an evolving area of policy and practice. Each country is on the second or third iteration of a national approach. As nations around the world experiment with different policies, laws, and organizational structures, cybersecurity will remain a dynamic policy environment, where best practices continue to evolve, guided by experience, new challenges, and the development of more sophisticated understanding by policy makers. The experiences of these countries provide a useful guide to best practices for other countries as they develop their own national approaches to cybersecurity.

This document, along with the 2016 Report "Cybersecurity: Are We Ready in Latin America and the Caribbean?" prepared by the Inter-American Development Bank and the Organization of American States, constitute the foundation for a separate study identifying the gap between the LAC region and these four recognized cases in the area of cybersecurity. This research can be found at: https://publications.iadb.org/handle/11319/7449 ■