CYBER READINESS INDEX 2.0

A PLAN FOR CYBER READINESS: A BASELINE AND AN INDEX

Principal Investigator: Melissa Hathaway

Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri

November 2015

POTOMAC INSTITUTE FOR POLICY STUDIES

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA, 22203
www.potomacinstitute.org
Telephone: 703.525.0770; Fax: 703.525.0299

Email: *CyberReadinessIndex2.0@potomacinstitute.org*

Follow us on Twitter:
@CyberReadyIndex

Acknowledgements

The Potomac Institute for Policy Studies would like to thank the International Telecommunications Union's ICT Applications and Cybersecurity Division, and the Organization of American States' Inter-American Committee Against Terrorism for their continuous support. The authors would also like to thank Sherry Loveless and Alex Taliesen for their editorial and design work.

CYBER READINESS INDEX 2.0

A PLAN FOR CYBER READINESS: A BASELINE AND AN INDEX

TABLE OF CONTENTS

CYBER READINESS INDEX 2.0

A PLAN FOR CYBER READINESS: A BASELINE AND AN INDEX

Principal Investigator: Melissa Hathaway
Chris Demchak, Jason Kerben,
Jennifer McArdle, Francesca Spidalieri

The Cyber Readiness Index 2.0 is expanded from the Cyber Readiness Index 1.0, published November 2013.

INTRODUCTION

Today, no country is cyber ready.

It is a given that global economic growth is increasingly dependent upon the rapid adoption of information communication technology (ICT) and connecting society to the Internet. Indeed, each country's digital agenda promises to stimulate economic growth, increase efficiency, improve service delivery and capacity, drive innovation and productivity gains, and promote good governance. Yet, the availability, integrity, and resilience of this core infrastructure are in harm's way. The volume, scope, velocity, and sophistication of threats to our networked systems and infrastructures are real and growing. Data breaches, criminal activity, service disruptions, and property destruction are becoming commonplace and threaten the Internet economy.

Global leaders understand that increased Internet connectivity leads to economic growth only if the underlying infrastructure and the devices connected to it are safe and secure. Therefore, countries must align their national economic visions with their national security priorities.

Until now, however, there has not been a comprehensive, comparative, experiential methodology to evaluate a country's maturity and commitment to securing its national cyber infrastructure and services upon which its digital future and growth depend. The Cyber Readiness Index (CRI) 1.0[1] represented a new way of examining the problem and was designed to spark international discussion and inspire global action to address the economic erosion caused by *cyber insecurity*.

Building on CRI 1.0, Cyber Readiness Index 2.0 examines one hundred twenty-five countries that have embraced, or are starting to embrace, ICT and the Internet and then applies an objective methodology to evaluate each country's maturity and commitment to cyber security across seven essential elements. By applying this methodology, a country can better understand its Internet-Infrastructure entanglements and the resulting dependencies and vulnerabilities.[2] Specifically, the CRI 2.0 assesses countries' levels of preparedness for certain cyber risks and identifies areas where national leaders can alter or refine their country's current posture by leveraging or changing laws, policies, standards, market levers (e.g., incentives and regulations), and implementing other initiatives to preserve the security of their connectivity and protect the value of their economy.

BACKGROUND

Most countries have embraced ICT-enabled economic strategies and are working to provide fast, reliable, and affordable communications to every household and business to move their information society into the digital age.[3] Modernization initiatives like e-government, e-banking, e-health, e-learning, next generation power grids, and automating elements of the transportation infrastructure and other essential services, are at the top of most countries' economic agenda. For example, China's Internet Plus strategy seeks to actively encourage the healthy development of e-commerce, industrial networks, and Internet banking, as well as facilitate the growth of new industries and the expansion of its companies' international Internet footprint.[4] Like many other countries, China views the Internet as key to its future growth and development opportunities. Similarly, India's Prime Minister Modi laid out his vision to transform his country into a "digitally empowered knowledge economy;" leveraging India's globally acclaimed information technology (IT) competence to create jobs in IT, telecommunications, and in electronic device markets. In addition, India is seeking to become an innovator in ICT solutions for health, knowledge management, and financial markets.[5] Finally, the European Commission is working to create a meaningful single market for digital services that can enable the free movement of goods, services, capital, and businesses. Successful implementation of this "Digital Single Market Strategy" is estimated to lead to an additional €415 billion per year in GDP growth across Europe.[6]

Countries must align their national economic visions with their national security priorities.

Governments, in developing countries in particular, are pushing for even more aggressive ICT adoption strategies to provide additional services to millions of citizens in order to more rapidly boost and deepen economic advances.[7] In fact, the World Bank estimates that for every 10 percent of the population connected to the Internet, GDP grows by 1 to 2 percent.[8] Moreover, recent research suggests a growing recognition among governments and businesses that embracing the Internet and ICTs will enhance their long-term competitiveness

and societal well-being, potentially contributing up to 8 percent of a nation's GDP.[9] Some reports go even further to suggest that the modernization of industrial systems (e.g., electric power grids, oil and gas pipelines, manufacturing, etc.) represents a 46 percent share of the global economy, and could rise to as much as 50 percent in the next ten years.[10]

Nations cannot afford to ignore this economic opportunity. But few are considering the impact and economic costs of less resilient critical services, exposure/violation of citizen privacy, theft of corporate proprietary data and state secrets, and the impact of e-fraud and e-crime—all of which lead to economic and national security instability. Put simply, cyber *insecurity* is a *tax* on growth.[11]

For example, it is estimated that the Group of Twenty (G20) economies have lost 2.5 million jobs to counterfeiting and piracy, and that governments and consumers lose up to $125 billion to cyber crime annually, including losses in tax revenue.[12] The United States estimates the annual impact of international intellectual property (IP) theft to the American economy at $300 billion. This corresponds to 1 percent of its GDP.[13] Other studies conducted by the Netherlands, United Kingdom, and Germany estimate similar losses in GDP. No nation can afford to lose even 1 percent of its GDP to illicit cyber activities. As countries continue to embrace ICT and Internet connectivity, however,

Cyber insecurity is a tax on growth.

Resilient connected societies must drive modernization with security at its core.

the exposure, attendant risks, and economic costs will exponentially increase if security and resilience are not at the core of their modernization strategies.

Measuring such losses to the economy will force national leaders to better align their country's national security agenda with their economic agenda and invest in the derivative value of both.[14] Bringing transparency to the economic losses caused by cyber insecurity may spark national and global interest in addressing this economic erosion. The CRI 2.0 establishes a framework to guide countries in securely pursuing the economic growth of a resilient, ICT-enhanced, and connected society.

CYBER READINESS INDEX 2.0 — THE METHODOLOGY

The CRI 2.0 has two main components: first, it is designed to inform national leaders on the steps they should consider to protect their increasingly connected countries and potential GDP growth by objectively evaluating each country's maturity and commitment to cyber security and resilience. Secondly, the CRI defines what it means for a country to be "cyber ready" and documents the core components of cyber readiness into an actionable blueprint for countries to follow. The CRI 2.0 methodology represents a useful, unique, and user-friendly tool to assess the gap between a nation's current cyber security posture and the national cyber capa-

bilities needed to achieve its economic vision. The blueprint developed and employed for this analysis includes over seventy unique data indicators across the following seven elements:

1. National strategy;
2. Incident response;
3. E-crime and law enforcement;
4. Information sharing;
5. Investment in research and development (R&D);
6. Diplomacy and trade; and
7. Defense and crisis response.

The fact-based assessments for each country rely on primary sources, and each unique data point is grounded on empirical research and documentation. Countries are assessed for each indicator across three levels of cyber readiness: insufficient evidence, partially operational or fully operational.

The CRI 2.0 methodology is being applied to evaluate one hundred twenty-five countries' cyber readiness; assessing each country's maturity and commitment to cyber security and resilient infrastructures and services (Figure 1 and Table 1).

The country selection includes the top seventy-five countries from the International Telecommunication Union (ITU) *ICT Development Index (IDI)* to emphasize the importance of connectedness. Members of the G20 economies were added because they represent 90 percent of global GDP, 80 percent of international trade, 64 percent of the world's population, and 84 percent of all fossil fuel emissions.

In order to be regionally representative and globally inclusive, additional countries were selected from: the Organization for Economic Cooperation and Development (OECD), the African Economic Community (AEC), the Latin American Integration Association (LAIA), the

Insufficient Evidence: evidence is lacking or has yet to be located. It is possible, however, that the data exists but is not yet publicly available or is classified.

Partially Operational: there is evidence of policies, activities, and/or funding, however, the activity may be immature, incomplete, or still in the early stages of development. While these initiatives can be observed, it may be difficult to measure their functionality.

Fully Operational: there is sufficient evidence to observe and measure a mature, functioning activity.[15]

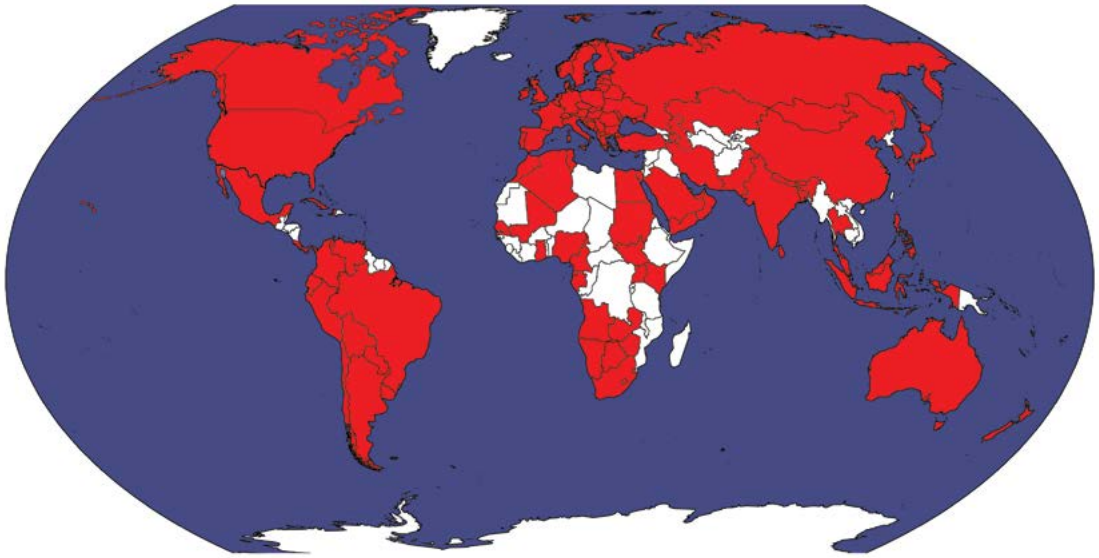

Figure 1: CRI 2.0 Country Selection

Algeria	Colombia	Israel	Netherlands	Sri Lanka
Andorra	Costa Rica	Italy	New Zealand	St. Kitts and Nevis
Angola	Croatia	Japan	Nigeria	St. Vincent and Grenada
Antigua and Barbados	Cuba	Kazakhstan	Norway	Sudan
Armenia	Cyprus	Kenya	Oman	Swaziland
Argentina	Czech Republic	Kyrgyz Republic	Pakistan	Sweden
Australia	Denmark	Latvia	Paraguay	Switzerland
Austria	Djibouti	Lebanon	Panama	Taiwan
Azerbaijan	Ecuador	Lesotho	Peru	TFYR Macedonia
Bahrain	Egypt	Lithuania	Philippines	Thailand
Bangladesh	Estonia	Luxembourg	Poland	Trinidad and Tobago
Barbados	Finland	Macau, China	Portugal	Tunisia
Belarus	France	Malaysia	Qatar	Turkey
Belgium	Gabon	Maldives	Romania	Uganda
Bhutan	Gambia	Mali	Russia	Ukraine
Bolivia	Germany	Malta	Saudi Arabia	United Arab Emirates
Bosnia & Herzegovina	Ghana	Mauritius	Senegal	United Kingdom
Botswana	Greece	Mexico	Serbia	United States of America
Brazil	Hong Kong	Moldova	Seychelles	Uruguay
Brunei Darussalam	Hungary	Mongolia	Singapore	Uzbekistan
Bulgaria	Iceland	Monaco	Slovakia	Venezuela
Cameroon	India	Montenegro	Slovenia	Vietnam
Canada	Indonesia	Morocco	South Africa	Yemen
Chile	Iran	Namibia	South Korea	Zambia
China	Ireland	Nepal	Spain	Zimbabwe

Table 1: CRI 2.0 Country Selection

Asia Pacific Economic Cooperation (APEC), the Central Asia Regional Economic Cooperation (CAREC), the Gulf Cooperation Council (GCC), the South Asia Association for Regional Cooperation (SAARC), and the North American Trade Federation. Countries from these regional economic groupings are represented in the IDI, and are often also included in the World Economic Forum's (WEF) *Network Readiness Index*. This ensures that every selected country is embracing ICT and investing in accessible and affordable Internet services to promote economic growth.

Given that the GCC is not representative of the Middle East, three states that have the highest GDP rankings outside the GCC were also added: Iran, Yemen, and Lebanon.[16]

This cross-section of one hundred twenty-five countries represents a significant portion of the world and is demonstrative of the diverse and representative nature of the CRI 2.0's country selection criteria.

The CRI 2.0's focus on the interconnection between economics and security (or lack thereof) provides a solid foundation for each country to assess its cyber security maturity, and serves as a framework for informing policy and strategy, operational and institutional initiatives, resourcing requirements, regulatory and legislative formulation, and diverse market lever implementation. Implementing CRI 2.0 will raise awareness about the linkage between a sustainable cyberspace and GDP growth for every country, given that the future of a country's GDP is likely to be increasingly technology dominated and Internet-related. Moreover, it creates the basis for understanding the economic erosion caused by cyber insecurity and the degree to which national security concerns are considered a component of a country's digital and economic agenda. This methodology can lead to analytically based decisions on how to respond to and get ahead of the problem.

Finally, the CRI 2.0 provides international entities, such as the ITU, the WEF, the Organization of American States (OAS), the Inter-American Development Bank (IDB), the World Bank, and others, with a framework and complimentary approach to their respective initiatives and international discussions.

A detailed description of the seven essential elements of the CRI 2.0 methodology follows. Each section contains an essential element with at least ten supporting indicators for evaluation that when combined represent a blueprint of a country's cyber readiness. Furthermore, country examples are provided that illustrate innovative and multicultural solutions towards becoming cyber ready. While these examples are by no means comprehensive, they do highlight unique country-level approaches.

1. NATIONAL STRATEGY

The first—*and most important*—area that indicates a country's cyber readiness is the articulation and publication of a National Cyber Security Strategy that aligns the country's economic vision with its national security imperatives. The Internet, broadband networks, mobile applications, IT services, software, and hardware constitute the foundations of the digital economy and a country's digital future.[17] The Internet and ICTs have become the backbone of family platforms (e.g., Facebook™, Twitter™, Insta-

gram™, Renren™, VKontakte™, etc.), business engines, critical services and infrastructures, and the global economy.[18] The inter-dependencies and hyper-connectivity touch each sector. For example, advanced manufacturing uses industrial control systems and robotics to increase productivity and decrease the need for manual intervention. Modern agriculture embeds Internet Protocol (IP) devices on crops to determine fertilizer requirements and to adjust water supplies. IP devices are also placed on livestock to determine where the animals graze and consume water, assessing the animals' health on a near-constant basis. E-commerce, the free flow of goods and services across borders, is displacing the role of traditional storefronts, delivering a wide variety of items directly to the doorstep of on-line shoppers shortly after they place an on-line order. Transportation systems now use sensors, mobile devices, and unmanned kiosks to manage traffic and deliver tickets. Connected cities use geo-location devices to track the speed and location of automobiles to determine if a driver has obeyed the laws of the road. Modernization initiatives in the healthcare industry are digitizing citizens' health records and employing cloud-based computing to enable swift access to healthcare records anywhere in the world. Telemedicine uses high-speed Internet to deliver medical advice and services to underserved areas. Finally, financial systems exchange trillions of dollars daily, commodities markets trade using digital currency, and Internet banking is replacing the need for local, physical banks.

The threats to networked infrastructures are on the rise. Countries are beginning to understand these threats and are outlining the need for infrastructure protection, data protection, defense of the homeland, and other descriptors. A comprehensive national cyber security strategy needs to describe the threats to the country in economic terms, and outline the necessary steps, programs, and initiatives that must be undertaken to address those threats and protect the Internet connectivity and the ICT utilized by citizens and private and public organizations.[19] The strategy should be underpinned by the economic potential of the Internet and ICT adoption and include the initiatives that will help reduce GDP erosion caused by cyber threats, as well as increase the security and resilience of the country as a whole.

National cyber security strategies must reflect the economic importance of cyber security.

A sound National Cyber Security Strategy must not be just articulated. It must be actionable. Today, the primary topics reflected in most strategies include: outlining organizational and positional authority within the government; fostering awareness and education among citizens; building an incident and crisis management response capability; expanding law enforcement's capacity to deal with the rate of cyber crimes; facilitating private-public partnerships and developing trusted information sharing exchanges; and marshaling resources toward a R&D and innovation agenda. Many strategies begin

with statistics, quantifying incident volume and the rate of infrastructure infection, and naming the variety of threats. The data is used to justify organizational responsibility and increased funding for missions and organizations. Rarely do these strategies prioritize the services and infrastructures that are most at risk, nor do they align the security measures and resource requirements necessary to reduce exposure and economic losses. A sound National Cyber Security Strategy should state the strategic problem or problems in economic terms; identify and empower the competent authority[20] that is accountable for the strategy's execution; include specific, measurable, attainable, result-based, and time-based objectives in an implementation plan; and recognize the need to commit limited resources (e.g., political will, money, time, and people) in a competitive environment to achieve the necessary security and economic outcomes.

At least sixty-seven countries (with others in development) have already published their cyber security strategy, outlining key steps that are intended to increase their national security and resilience.[21] Many others have national strategies (not specific to cyber security) that guide and coordinate their efforts to advance their cyber security posture. Few countries, however, are explicitly linking their economic and national security agendas and specifically addressing the economic importance of cyber security. Fewer still are building actionable strategies. Therefore, all countries have an opportunity to revise or develop their strategies to reflect the economic importance of cyber security.

Elements of a comprehensive national cyber security strategy should include:

Statement:

A. The publication of a national cyber security strategy that is inclusive of economic opportunities and risks associated with ICT uptake;

Organization:

A. The designation of a competent authority and the clear delineation of its positional authority;

B. The identification of the key government entities affected by, and/or responsible for, the implementation of the national cyber security strategy;

C. The identification of commercial-sector entities affected by, and/or, responsible for the implementation of the national cyber security strategy (recognizing commercial-sector dependencies);

Resources:

A. The identification of the financial and human resources requested and allocated for the implementation of the strategy;

B. The identification of the percentage of GDP expected to be gained or lost (grossly) by implementing the strategy;

Implementation:

A. The identification of the mechanisms required to secure critical cyber infrastructure and ICT uptake;

B. The identification of critical services (not critical infrastructures) that the strategy intends to make more secure and resilient; and

C. The identification of national standards for continuity of service agreements (24 hours/7 days a week) and outage reporting requirements for each critical service, industry, and infrastructure.

The findings in this essential element, as with the other six areas, represent a snapshot in time of a dynamic and changing landscape. As countries continue to develop their national cyber security strategies, updates to this essential element will reflect those changes and monitor, track, and evaluate substantive and notable developments. Thus, the CRI 2.0 will continue to provide a blueprint with new examples to inform others in the formulation or revision of their strategies.

2. INCIDENT RESPONSE

The second essential element that indicates a country's cyber readiness involves establishing and maintaining an effective national incident response capability. Often, this capability takes the form of one or more National Computer Security Incident Response Teams (National CSIRTs) or Computer Emergency Response Teams (CERTs)—hereinafter referred to collectively as CSIRTs—responsible for managing incident response in the event of natural or man-made cyber-related disasters that affect critical services and information infrastructures.[22] At present, one hundred and two national CSIRTs have been established worldwide and another four CSIRTs are under development.[23] CSIRT teams usually consist of a blend of IT security experts and practitioners from academia, the private sector, and government. In addition to providing the specific technical competence to respond to cyber incidents of national interest, these incident response teams strengthen the ability of a national government to understand and combat cyber threats. Operating a National CSIRT, therefore, forms a core component of a country's overall strategy to secure and maintain the services and infrastructures that are vital to national security and economic growth.[24]

National CSIRTs, unlike strictly governmental ones, serve a broad constituency ranging from government departments to private and public entities to citizens. A well-established National CSIRT provides reactive services above all else—i.e., the ability to respond to incidents by containing and mitigating incidents as they occur.[25] Although the specific organizational form of National CSIRTs may vary, and not every country may have the same needs and resources, these specialized and dedicated units should provide a series of both proactive and reactive functions, as well as preventive, educational, and security quality management services. These services include, but are not limited to: establishing shared understanding of the threats facing the country; publishing alerts and advisories on cyber vulnerabilities and threats; promoting cyber security awareness and best practices; identifying, detecting, containing, and managing security threats and preparing for potential incidents; coordinating incident response activities; analyzing computer security incidents and providing feedback and lessons learned (for shared learning); promoting activities that increase resilience; and supporting the national cyber security strategy.

For example, Singapore's national CSIRT (SingCERT) was developed by the Infocomm Development Authority of Singapore (IDA) in cooperation with the National University of Singapore (NUS) in 1997. It has since become a part of the Cyber Security Agency of Singapore (CSA). SingCERT was designed as a one-stop center for incident response; facilitating the detection, resolution, and prevention of security related incidents on the Internet. SingCERT provides technical assistance and coordinates response to cyber security incidents, identifies and follows cyber intrusion trends, disseminates timely threat information, and coordinates with other security agencies to resolve computer security incidents.[26] SingCERT has also been active in organizing and hosting Association of South East Asian Nations (ASEAN) and Asia Pacific Computer Emergency Response Team (APCERT) exercises. Additionally, Singapore hosts seven Forum of Incident Response and Security Teams (FIRST) members.

Brazil's incident response capabilities consist of a national computer emergency response team, *CERT.BR*, and thirty regional CSIRTs split across four states, all under the authority of the Brazilian Internet Steering Committee. This Committee is a non-governmental, multi-stakeholder organization and the primary entity responsible for network defense and incident response in Brazil.[27] Brazil's *CERT.BR* is responsible for incident response, awareness raising, data collection on cyber threats and intrusions, and coordination with multiple stakeholders to include CSIRTs, academia, and the private sector. In addition, Brazil's CSIRTs include teams from the financial sector, military, government, and universities.[28]

Apart from national CSIRTs, similar regional entities have been established to enhance and coordinate incident response activities within specific geographic regions. AfricaCERT, for instance, is a non-profit organization that includes eleven African countries and provides a forum for cooperation and the exchange of technical information between operators of Internet-connected networks in the region. AfricaCERTs main objectives include, but are not limited to: coordinating cooperation among African CSIRTS to handle computer security incidents; assisting in the establishment of CSIRTs in countries that currently lack incident response capabilities; fostering and supporting incident prevention and educational outreach programs in ICT security; encouraging information sharing; and promoting best practices for cyber security. Similarly, the APCERT comprises a network of twenty-eight member CERTs and other trusted security experts in the region, and it aims to enhance awareness and competency in relation to computer security incidents and improve incident response

Resilience of critical services is vital to national security and economic growth.

capabilities across the Asia Pacific region.[29] APCERT's mission is the pursuit of a "clean, safe, and reliable" cyberspace through global collaboration. In order to effectively communicate cyber threats, APCERT's organizational framework relies on a point-of-contact (POC) system, in which each country delegates an APCERT member to serve as a POC during times of emergency, in order to help facilitate timely response.[30] Likewise, the Organisation of Islamic Cooperation Computer Emergency Response Team (OIC-CERT)—which includes member states in Southeast Asia, South Asia, the Middle East, Africa, and Central Asia—also works to enhance collaboration between member state CERTs and OIC-CERT.

In addition to developing incident response capabilities, countries are also participating in cyber incident response exercises. These exercises help countries practice and develop skills for effective crisis management and verify the operational ability of a CSIRT to respond under pressure. For example, in November 2011, the German Executive Branch conducted a one-day crisis planning/readiness exercise. The goal of the exercise was to work out government response procedures for a multi-pronged attack that included: distributed denial of service (DDoS) attacks against critical infrastructures; the injection of malware into the banking system, causing a crisis with ATMs and credit cards; and the insertion of false traffic within the air traffic control system.[31] The Swedish Civil Contingencies Agency (MSB), the Post and Telecom Authority (PTS), and the National Defence Radio Establishment (FRA) also host regular cooperative Chief Information Assurance Officer (CIAO) courses for relevant employees working at the senior management levels. The course culminates in a capstone exercise—a cyber crisis management simulation—that includes key public and private stakeholders in the decision making process, to include Parliament and Chief Executive Officers (CEOs) from companies responsible for Swedish critical services. The exercise highlights crucial policy and legal shortfalls, while at the same time educating all participants on cyber security.[32] Additionally, the Czech Republic conducted an incident response exercise in October 2015 that focused on threats to critical infrastructure, with a specific emphasis on nuclear power plants.[33] Some countries are also conducting exercises in reaction to cyber incidents that have occcured. For example, South Korea's President Park Geun-hye ordered cyber war drills and training for all staff, as a result of malware found in multiple Korea Hydro and Nuclear Power (KHNP) plants.[34]

Furthermore, international exercises test operational incident response capabilities while simulating cooperation between countries. The United States, for example, conducts a biannual Cyber Storm exercise that seeks to strengthen cyber preparedness in the public and private sectors. Each Cyber Storm exercise builds on lessons learned from previous real-world incidents, to ensure that participants have an opportunity to practice incident response to ever-more sophisticated cyber incidents. The 2016 Cyber Storm will include sixteen states, eleven countries, and fourteen federal agencies.[35] The European Union also holds biannual cyber incident response exercises among member states and the private sector, entitled Cyber Europe.[36] During a 24 hour cyber exercise in 2014, Cyber Europe allowed nearly all European Union member states to test their response capabilities against as many as two thousand real-life cyber attacks, to include DDoS, web defacement attacks, data exfiltration, and cyber attacks against critical infrastructure.[37] Moreover, the European Defense Agency (EDA) and the North America Treaty

Organization (NATO) also conduct region wide complex cyber crisis management exercises, with the goal of strengthening cyber incident response capacity among member states and understanding cross-border dependencies.[38] The United States and the United Kingdom also recently announced that they will test how financial centers on either side of the Atlantic would respond to a massive cyber attack. The exercise ran in November 2015 and tested country response and cross-Atlantic coordination and communication.[39]

National CSIRTs can also be used as a mechanism to build confidence between countries and foster cooperation. For example, China, Japan, and Korea—three countries that have historically experienced tensions—have developed a trilateral annual CSIRT meeting to discuss cyber incident response mechanisms. The meetings have helped instill confidence and trust resulting in the development of a cyber "hotline" to communicate on significant cyber incidents.[40]

Cyber incident response capabilties, joint meetings, and exercises are just a few of the basic mechanisms that can help a country proactively prepare for and mitigate the ripple effects of a major cyber incident. CSIRTs increase a country's speed, recovery, and resilience against cyber threats, reducing the likely overall economic and operational impact of nationally significant attacks or campaigns. Some of the key preconditions for the successful deployment of these incident response teams are a well trained staff, and effective rapidly deployable tools. This facilitates an incident response team's ability to foster cooperation and coordination in incident prevention, enable rapid reaction to incidents, and promote information sharing among stakeholders, both domestically and internationally.

Elements of a sound national incident response capability should include:

Statement:

A. The publication of an incident response plan for emergencies and crises;

B. The identification and mapping of cross-sector dependencies that address continuity of operations and disaster recovery mechanisms;

C. Evidence that the plan is exercised and updated regularly;

D. The publication and dissemination of a national cyber threat assessment(s) on government, critical infrastructures, and essential services networks;

Organization:

A. The establishment of a national CSIRT to manage incident response and serve a broad national constituency (beyond government and critical infrastructure providers);

B. The identification of a network of authoritative national contact points for governmental and regulatory bodies;

C. The identification of a network of authoritative national contact points for critical industries that are essential for the operation and recovery of critical services and infrastructures;

D. The development of an information warning and alert system that can be used by national crisis/response centers to effectively receive, address, and transmit urgent information in a timely manner;

Resources:

A. The identification of the financial and human resources requested and allocated for the National CSIRT to carry out its mandate;

B. The identification of additional funding to activate and regularly test the information warning and alert system, and to measure the country's resilience to cyber incidents and crisis through national cyber security exercises;

Implementation:

A. A demonstrated capability in the incident containment, management, resilience, and recovery processes for critical services and infrastructures;

B. A demonstrated ability by national crisis/response centers to address and transmit alerts in a timely manner;

C. Evidence of ongoing research methods analyzing trends or groups of computer security incidents of national concern—sharing similar actors or tactics, techniques, and procedures—in order to identify patterns; and

D. The development and implementation of a system/program to regularly test and measure the nation's resilience to cyber incidents and crises through national cyber security exercises.

Initial findings in this essential element are based on the inventories of National CSIRTs provided by the CERT Division at Carnegie Mellon University (CMU),[41] the European Network and Information Security Agency (ENISA),[42] FIRST,[43] and the ITU. Additional primary and secondary sources, such as National CSIRT's websites and related news articles, are consulted to determine if the capabilities exist and are funded. As countries come to recognize the importance of establishing National CSIRTs, updates to this essential element will monitor, track, and evaluate those developments.

3. E-CRIME AND LAW ENFORCEMENT

The third essential element that indicates a country's cyber readiness is demonstrated through its commitment to protect its society against cyber crime. Cyber crime is not simply a domestic issue; it transcends national borders and therefore requires transnational solutions. Countries must show an *international* commitment to secure society against e-crime. Most often, this capability takes the form of involvement with international fora dedicated to addressing international cyber crime issues, as well as the establishment of domestic legal and regulatory mechanisms to combat cyber crime. The pertinent legal and regulatory authorities designated with carrying out such activities should define what constitutes a cyber crime and empower governmental entities with the mechanisms, expertise, and resources to investigate and effectively prosecute cyber crime activities.

Two international treaty agreements help demonstrate a country's commitment to protecting society against cyber crime: the Council of Europe's "Convention on Cyber Crime" and the Shanghai Cooperation Organisation's "Agreement on Cooperation in the Field on Ensuring International Information Security". The Council of Europe's "Convention on Cybercrime", in force since July 1, 2004 and

commonly called the *Budapest Convention*, provides a mechanism through which to harmonize divergent national cyber crime laws and encourage law enforcement collaboration.[44] The effectiveness of the Budapest Convention is somewhat limited because it allows signatory countries to selectively implement elements of the Budapest Convention based upon findings that doing otherwise would "prejudice its sovereignty, security, public order or other essential interests."[45] The Shanghai Cooperation Organisation's "Agreement on Cooperation in the Field on Ensuring International Information Security," signed in 2009 and sometimes referred to as the Yekaterinburg Agreement, has principles consistent with the law enforcement approach of the Budapest Convention. It too seeks to improve the informational legal base and establish practical mechanisms of cooperation among the parties in ensuring international information security.[46] Pursuant to these treaties, countries agree to adopt appropriate legislation, foster international cooperation, and combat criminal offenses, by facilitating their detection, investigation, and prosecution both nationally and internationally. CRI 2.0 credits countries that have ratified or acceded to either of these treaties because by doing so a country has a specific obligation and duty under its domestic law to uphold a commitment in an international context.

In addition to the international mechanisms noted above, other international, multi-national, and regional approaches towards addressing international cyber crime exist and are being pursued. For example, the United Nations General Assembly (UNGA) has passed a variety of resolutions relevant to cyber crime, such as the 2001 "Combating the Criminal Misuse of Information Technology," and the 2003 "Creation of a Global Culture of Cybersecurity and the Protection of Critical Infrastructures."[47] Notably, the UN Group of Government Experts (GGE) that consists of twenty countries had a break through moment when they agreed to cooperate on prosecuting terrorist and criminal use of ICT. Their commitments are codified in the June 2015 GGE report *On Developments in the Field of Information and Telecommunications in the Context of International Security*.[48] The APEC also conducted a capacity-building project on cyber crime for member economies to establish legal structures and build capacity to investigate e-crime. As part of this project, advanced APEC economies support other member-economies by training legislative authorities and investigative personnel.[49]

The CRI 2.0 draws upon these international, multi-national, and regional approaches to assess a country's cyber readiness. In addition, the CRI 2.0 also includes country information on cyber crime from the ASEAN, and the ITU, among others.

While the intention to cooperate on cyber crime may exist and the ratification of cyber crime agreements is important, it does not necessarily demonstrate readiness to combat cyber crime. States must also work to proactively build domestic cyber law enforcement capacity. For instance, the Advanced Centre for Research, Development and Training in Cyber Law and Forensics at the National Law School of India University in Bangalore works to translate the law into technical terms and vice-versa by providing training and education to judicial officers, prosecutors, investigative agencies, cyber security personnel, technologists, and others. Funded by the Department of Electronics and Information Technology (DeitY) in the Indian Ministry of Communications and Information Technology, the Centre provides a unique hands-on training component

in a cyber forensics lab that facilitates rapid understanding of complex issues.[50]

Another example is the International Police Organization's (INTERPOL) recent launch of an INTERPOL Global Complex for Innovation (IGCI) in Singapore. This facility enables law enforcement officials to partner with industry to develop new training techniques and use advanced tools to tackle cyber crime and boost cyber security.[51] For example, INTERPOL created a simulation game to teach law enforcement officials about the intersection and risk of the Darknet and crypto-currencies. The Darknet has enabled an underground (illegal) economy that sells personal identifiable information (PII), military intelligence, weapons designs, modular malware, zero-day exploits, private encryption keys and credentials, and many other types of illegally obtained data. INTERPOL's first simulation/training exercise was conducted in July 2015.[52]

Apart from building e-crime and law enforcement capacity, states must also work to clean the infections in their networked infrastructures, known as botnets.[53] Currently, an estimated five to twelve percent of computers worldwide are compromised as a part of a botnet network. The FBI estimates that eighteen systems are infected per second via botnet armies, causing an estimated $110 billion in damages globally.[54] Some countries have worked to address this threat, with some success. For example, the Canadian Government's DarkSpace Project-*Advanced Analytics and Dark Space Analysis for Predictive Indicators of Cyber Activity*—spearheaded by Bell Canada and involving a team of experts from Canadian government agencies, academic institutions, and industry—made a business case for a 'clean pipes' solution to cyber threats by providing a compelling body of evidence to support proactively containing threats to Canada coming from the Internet. Findings from the project made the business case for a national clean pipes strategy and influenced a Cyber Security Standard for Telecommunications Service Providers.[55] Another example, in Japan, was The Cyber Clean Center, a five-year funded effort, operated by the Japanese CERT (JPCERT) from 2006 to 2011.[56] This Center was the result of a cross-disciplinary collaboration among JP-CERT, various security vendors, and Internet service providers (ISPs); it created an automated "guardian network" against botnet malware infection and exploitation. It also further provided tailor-made solutions to address specific malware on specific computers.[57] The Cyber Clean Center's efforts have continued at Telecom-ISAC Japan.[58] Finally, Australia's iCode, a public-private partnership through the Australian Internet Security Initiative (AISI), aims to promote a security culture among ISPs by reducing the number of compromised computing devices in Australia. The iCode encourages all Australian ISPs to

Reducing the number of infected networked devices is an important investment in combatting e-crime.

Cyber crime and fraud are a tax on economic growth.

join AISI, and provides AISI ISP members with daily malware infection and service vulnerability data.[59]

Cyber crime and fraud are a tax on economic growth. Cyber crime has reached an estimated $445 billion worldwide, with a negative impact on national economies of at least 1 percent of GDP and upwards of two hundred thousand lost jobs.[60] An investment in combating cyber crime and increasing law enforcement capacity is a necessary investment for the economy. By developing law enforcement capabilities to fight e-crime through the ratification of treaty documents, international cooperation, capacity development, the implementation of anti-botnet programs, and other initiatives, countries can mitigate their cyber risks and boost future economic growth.

Essential elements of a sound country-level and international commitment to protecting society against cyber crime should include:

Statement:

A. A demonstrated national and international commitment to protect society against cyber crime through ratifying international cyber crime agreements or other equivalent agreement to fight cyber crime;

B. A demonstrated commitment to establish national legal and policy mechanisms to specifically reduce the criminal activity emanating from the country and promote coordination mechanisms to address international and national cyber crime;

Organization:

A. The establishment of a mature institutional ability to fight cyber crime, including training for court judges, prosecutors, lawyers, law enforcement officials, forensic specialists, and other investigators;

B. The establishment of a coordinating agency with a primary mission and authority to ensure that all international cyber crime requirements are being met domestically and across jurisdictional lines (i.e., cross-border cooperation);

Resources:

A. The identification of financial and human resources requested and allocated for fighting cyber crime;

B. The establishment of an accounting mechanism to determine what percentage of annual GDP is affected by cyber crime (actual loss in real currency), in order to assess national systemic cost-benefit tradeoffs and allocate resources accordingly;

Implementation:

A. Demonstrable evidence of a country's commitment to review and update existing laws and regulatory governance mechanisms, identify where gaps and overlapping authorities may reside, and clarify and prioritize areas that require modernization (e.g. existing laws, such as old telecommunications law);

B. The establishment of criminal offenses under domestic law for actions directed against the confidentiality, integrity, and availability of computer systems, networks, and computer data as well as the misuse of such systems, networks, and data, to include the international infringement of copyright; and

C. Demonstrable evidence of a country's effectiveness in reducing infections emanating from its own infrastructures and networks (e.g. creation of anti-botnet and malware remediation initiatives).

Initial findings in this essential element are based upon a review of whether a country has ratified or acceded to the Budapest Convention or the Shanghai Cooperation Organisation's Yekaterinburg Agreement and whether the country is an active participant in regional, multi-national, or international approaches towards addressing cyber crime. Additionally, current botnet activity (both command and control nodes and total infections) emanating from the country is used to assess the effectiveness of anti-botnet initiatives. The CRI 2.0 draws on primary and secondary sources to determine whether a country has established legal and regulatory mechanisms, other risk reduction activities, and allocated funding to ensure successful execution. Updates to this essential element will monitor, track, and evaluate substantive and notable developments.

4. INFORMATION SHARING

The fourth element that indicates a country's cyber readiness is its ability to establish and maintain information sharing mechanisms that enable the exchange of actionable intelligence and/or information between governments and industry sectors. Key activities such as identifying, assessing, and responding to targeted attacks—which can have significant implications for global telecommunications, trade, and business—requires more than traditional monitoring and protection mechanisms. Globally, most governments and organizations have established information sharing programs to better understand risks posed by state and non-state actors and managed their exposure to vulnerabilities and subsequent infections and breaches.

Formal information sharing mechanisms, similar to some of the services provided by National CSIRTs and CERTs, can help foster coordination in incident response, facilitate real-time sharing of threat and intelligence information, and help improve understanding of how sectors are targeted, what information is lost, and what methods can be used to defend information assets. At least four different models for information sharing have emerged to address cyber threats and to help entities secure their information assets: (1) government driven; (2) industry driven; (3) non-profit-partnership driven; and (4) a hybrid academic-, government-, and industry-partnership driven model. Each method has its unique challenges, such as balancing the need for exchanging timely and actionable cyber security information while protecting data's confidentiality, safeguarding civil liberties, and managing competing financial and human resources and interests. Two factors, however, are required for any of the four models to succeed: buy-in and trust, which must be underpinned by clearly defined objec-

Information sharing must be underpinned by trust and buy-in from all stakeholders.

tives, roles, responsibilities, and outcomes. Put simply, when a party participates reluctantly or defensively, success is hard to achieve.[61]

Moreover, stakeholders must be able to share valuable information on serious incidents, which requires clear definitions of what type of information should be shared, who will have access to it, and what security measures should be taken to protect the information once released by its original owner. The complexity of this sensitive information exchange grows proportionately with group size, and perhaps exponentially when those group members are sovereign states with distinct national security concerns.

Many individual countries have already developed strong national information sharing programs that could be leveraged as good practices for other countries to learn from. These programs tend to focus on aligning similar stakeholders into groups and subsequently aligning the groups into a national program. The Netherlands, for instance, created the National Cyber Security Centre (NCSC)—a government driven initiative that evolved from the Dutch GOVCERT into a successful public-private partnership—responsible for digital security and information sharing in the country.[62] One of its main tasks is to continuously monitor all (potentially) suspect sources on the Internet and alert public authorities and organizations of any identified cyber threat. NCSC is also directly connected to all Information Sharing and Analyses Centres (ISACs) in the country and information is shared under the Traffic Light Protocol (TLP), which classifies information into four levels: red, yellow, green, and white. The Dutch information sharing program was modeled after the United Kingdom National Infrastructure Security Coordination Centre (NISCC), which delivered focused information security advice to critical national infrastructure businesses.[63] Similarly, Japan's Information-Technology Promotion Agency (IPA), acts as the institutional authority charged with sharing information between government and critical industries, and has a proven track record establishing trusted relationships with all major companies in the country and providing timely and effective intelligence. In addition, IPA works closely with the Ministry of Economy, Trade, and Industry (METI), the National Information Security Center (NISC), and the Cyber Rescue Advice Team (J-CRAT) to respond to all major cyber incidents affecting critical infrastructure.[64]

Alternatively, in the United States, the Financial Services Information Sharing and Analysis Center (FS-ISAC)—an industry driven initiative developed by the financial services sector—helps facilitate the detection, prevention, and response to cyber incidents and fraud activity. It has built strong ties with financial service providers; commercial security firms; federal/national, state, and local government agencies; law enforcement; and other trusted entities to provide reliable and timely cyber threat alerts and other critical information to member firms worldwide. As part of these efforts, FS-ISAC uses a different Traffic Light Protocol to determine which audiences can and should receive specific information.[65] FS-ISAC is expanding its threat information sharing internationally to the United Kingdom and Europe. Other ISAC's also exist across many sectors, however are not as effective.

The National Cyber-Forensics and Training Alliance (NCFTA) in the United States is a non-profit

corporation with a mission to facilitate collaboration among private industry, academia, and law enforcement to identify, mitigate, and neutralize complex cyber-related threats. In addition to state and local law enforcement and industry representatives, this non-profit partnership-driven initiative enjoys international representation from Canada, Australia, United Kingdom, India, Germany, the Netherlands, Ukraine, and Lithuania. NCFTA provides streamlined and timely exchange of cyber threat intelligence to corporations, and also partners with subject matter experts in the public, private, law enforcement, and academic sectors to mitigate risks and fraudulent activities and gather the evidence necessary to prosecute criminals.[66]

Real-time actionable information is key to mitigating cyber threats.

Finally, Norway's Center for Cyber and Information Security (CCIS) at Gjøvik University College is a joint initiative (academia, government, and industry) and represents another approach to information sharing and collaboration on cyber security. CCIS promotes a systematic country-wide approach to cyber and information security and provides information sharing schema to safeguard society's ability to detect, alert, and handle serious cyber incidents. Additionally, it supports high quality national research and development of solutions in the field of cyber and information security.

In addition to the various information sharing programs that countries are developing, most governments' defense and intelligence agencies collect valuable cyber-related information, and some have started to declassify this type of intelligence and share it with other government entities and critical industries. Indeed, real-time situational awareness is often key to prevent or mitigate specific cyber threats. Some countries, such as Brazil, have devised mechanisms to declassify (write-for-release) actionable information alerting other entities (public and private) to vulnerabilities, specific threats and tactics, and potential defensive solutions as part of their information sharing initiatives.[67] Enhancing the defensive posture of the country is essential and some countries are willing to declassify portions of intelligence to better ensure security.

The ability of a country to exchange timely, accurate, and actionable information—within and between public and private sector entities—helps reduce vulnerabilities and exposure that can subsequently reduce attendant risks. As information sharing increases in frequency and quality, entities should be able to address cyber threats to their networked infrastructures in a faster and more proactive manner. Establishing and maintaining actionable information sharing programs is a fundamental investment for economic growth.

Elements of an effective national, cross-sector, and actionable information sharing program should include:

Statement:

A. The articulation and dissemination of a policy on information sharing across sectors that enables the exchange of actionable intelligence/information between governments and industry sectors;

Organization:

A. The identification of an institutional structure that transmits authoritative information from government sources to government agencies and critical industries (Government-to-Government);

B. The identification of an institutional structure that ensures that mechanisms exist (reporting schema, technology, etc.) for cross-sector incident information exchange (bi-directional), both operational (near-real-time) and forensic (post-facto) (Government-Industry/Industry-Industry);

C. The establishment of an academic or non-profit driven mechanism for vulnerability, incident, or solution information exchange (alternative model, for example, NCFTA or the National Vulnerability Database);[68]

Resources:

A. The identification of the financial and human resources requested and allocated for the government driven authoritative information exchange or other institutional structure(s) dedicated to the information sharing mechanisms;

Implementation:

A. Demonstrable evidence that cross-sector and cross-stakeholder coordination mechanisms meant to address critical interdependencies—including incident situational awareness and cross-sector and cross-stakeholder incident management—are adequately maintained and tested for effective performance; and

B. Demonstrable evidence of the ability and timely processes for the government to declassify (write-for-release) usable cyber-related intelligence information and share it with the rest of government and critical industries.[69]

Initial findings in this essential element are based upon a review of whether a country has established information sharing and other coordination mechanisms. Drawing upon primary and secondary sources, the CRI 2.0 determines whether such mechanisms exist and are properly funded. Updates to this essential element will monitor, track, and evaluate substantive and notable developments.

5. INVESTMENT IN RESEARCH AND DEVELOPMENT

The fifth element that indicates a country's cyber readiness is establishing a national priority for and investment in cyber security basic and applied research and ICT initiatives broadly. Advances in ICT have revolutionized almost every sector of the economy, transforming businesses, governments, education, and the way citizens live, work, and play. These innovations drive economic growth and can enhance resilience and set the conditions for a strong security posture.

Government and businesses each have a role to play and can combine the power of their R&D budgets to enhance the next generation of ICT and Internet-enabled technologies and solutions. Businesses and governments are embracing mobile Internet, cloud computing, big data, quantum computing, and the Internet of Things (IoT), and must invest in the trust, security, and resilience of these digital services and technologies. By investing in cyber R&D and

other innovations, countries, universities, and companies can improve their ability to close the gap between their cyber insecurity and attacker capabilities. For example, the European Union's Horizon 2020 program has allocated an estimated €80 billion for research and technological development initiatives. With the European Union's foundational principle of open access, the program intends to boost research results, accelerate innovation, create greater efficiency, and improve transparency. Horizon 2020 has three main components. The first area focuses on basic and applied science, entitled, "Excellent Science," and plans to fund doctoral training for an additional twenty-five thousand PhD candidates during the next seven years. The second area focuses on "Leadership in Enabling and Industrial Technologies," with an emphasis on ICT, nanotechnologies, advanced materials, and processing, among others. The third area funds solutions to address social and economic problems, such as health, energy, transportation, and security. One of the evaluation criteria for this investment is transnational cooperation among companies and solutions that meet pan-European needs.[70]

Cyber security R&D innovation must enhance the trust, security, and resilience of our future networked society.

Similarly, the United States prioritizes, coordinates, and dedicates over $4 billion annually toward cross-cutting research through the National Information Technology and Research and Development (NITRD) program. Priority research areas for 2016-2020 include: big data, cyber-physical systems, cyber security and privacy R&D, high-end computing, and wireless-spectrum sharing.[71] The NITRD program is the United State's primary source of federally funded work on advanced information technologies in computing, networking, and software. The program seeks to accelerate the development and deployment of advanced information technologies to enhance national defense and homeland security as well as improve United States productivity and economic competitiveness. Additionally, the Defense Advanced Research Projects Agency (DARPA), the Intelligence Advanced Research Projects Activity (IARPA), and the Homeland Security Advanced Research Projects Agency (HSARPA) also have funding dedicated to cyber R&D. However, if the entire cyber R&D budget were to be added together, the total amount would still be the equivalent of less than 1 percent of United States GDP. Based on the enormity of current and future United States cyber risks, 1 percent of GDP is inadequate to close the cyber insecurity gap.

Other government-sponsored initiatives encourage cyber security innovation by offering market incentives such as R&D tax credits. For instance, recognizing that spurring organizational and corporate investment often requires government encouragement and commitment, Israel recently approved significant tax breaks for cyber defense companies that join and establish activities at their national cyber park in Be'er Sheva.[72] By encouraging a unique industry-academia-military ecosystem through the co-location of technical talent, Israel is creating an economic and strategic cyber security hub. Be'er Sheva's cyber park also increases private-public partnerships in the cyber field; serves as a center of excellence for innovation; and provides an effective training and employment pipeline.

Grants and scholarships are another market mechanism used to advance cyber security education, develop knowledge, and build skills. For instance, the Brazilian government's "Science without Borders" program offers scholarships in all STEM fields, including computer science and information technology. Likewise, the National Council for Scientific and Technological Development (CNPq), an agency within the Ministry of Science, Technology, and Innovation, provides a "Science Initiation Scholarship" to incentivize ICT education in young students.[73]

Cyber Innovation hubs accelerate the transfer of ideas and technologies into solutions.

Cyber security innovation centers, such as the Hague Security Delta (HSD), foster innovative cyber security R&D and promote collaboration among private sector companies, governments, and research institutions. HSD, a foundation supported by the Municipality of the Hague and the Dutch Ministry of Economic Affairs, is the largest security network in Europe with knowledge bridges to the main security networks in the United States, Canada, Singapore, and South Africa. Its cyber security program includes initiatives such as the Cyber Security Academy and the Cyber Incident Experience Lab. Current projects include building an advanced malware detection platform and delivering solutions for detecting, reporting, and managing cyber vulnerabilities through qualitative scanners.[74]

Other private sector "cyber innovation hubs" have emerged in Silicon Valley, Tel Aviv, Boston, New York City, and London. For instance, London's cyber innovation hub, titled CyLon or Cyber London, is Europe's first cyber security startup accelerator. CyLon works to foster the cyber innovation ecosystem in London and helps businesses develop information security related products.[75]

These various R&D initiatives and cyber innovation hubs accelerate the transfer of ideas and technologies into solutions to advance the digital marketplace, improve the security and resilience of underlying networks and infrastructures, and improve societal well being.

Elements of a country's commitment to advance its cyber R&D, education, and capacity building efforts should include:

Statement:

A. A publicly announced commitment by the government to invest nationally in cyber security basic and applied research;

B. Publicly announced incentive mechanisms (e.g., R&D tax credit) to encourage cyber security innovation and dissemination of new findings, baseline technologies, techniques, processes, and tools;

C. Publicly announced government incentive mechanisms (e.g., grants, scholarships) to encourage cyber security education, knowledge creation, and skills development;

Organization:

A. The identification of at least one entity with the responsibility to oversee national cyber security R&D initiatives and serve as a national and international point-of-contact for collaboration;

B. The establishment of institutionally supported degree programs in cyber security, information security or similar advanced technology areas that focus on security and resilience of the digital environment;

C. The establishment of an entity with the mission to measure and report on the rate of government or commercial successfully transitioned programs (from research to product/service) with a focus on the solutions that improve security and resilience of the digital environment;

Resources:

A. The identification of financial and human resources requested and allocated for cyber security basic and applied research and initiatives;

B. The identification of financial and human resources requested and allocated for commercial or government transfer of enhanced technology and innovation;

Implementation:

A. The implementation of programs dedicated to the development, dissemination, and routinization of interoperable and secure technical standards, acceptable to and reinforced by internationally recognized standards bodies;

B. Evidence of national government efforts to support, advance, and sustain cyber security R&D, especially as demonstrated in terms of the research/production conversion rate (e.g., percentage implemented operationally within the government) and of the commercial adoption rate of successfully transitioned programs; and

C. Evidence of additional commercial efforts (e.g. cyber innovation hubs) to support, advance, and sustain cyber security R&D, especially in terms of the research/product conversion rate (e.g. percentage implemented operationally within the private sector) and of the government adoption rate of successfully transitioned programs from the commercial sector.

Initial findings in this essential element are based upon a review of whether a country is investing in cyber R&D, education, knowledge creation, and skills development—in addition to funding cyber security initiatives more broadly. Drawing on primary and secondary sources, the CRI 2.0 determines the type, if any, of government incentive mechanisms already in place and the resources dedicated to initiatives similar to the ones discussed above. Updates to this essential element will monitor, track, and evaluate substantive and notable developments.

6. DIPLOMACY AND TRADE

The sixth essential element of cyber readiness is demonstrated through a country's engagement with cyber issues as part of its foreign policy. At a fundamental level, cyber diplomacy seeks to find mutually acceptable solutions to common challenges. Cyber issues are emerging in many different international relations areas including human rights, economic development, trade agreements, arms control and dual use technologies, security, stability, and peace and conflict resolution. While cyber security issues are entangled in almost every topic and most negotiators are experts in a specific topic area (i.e., trade or arms control), those experts are often not familiar with the added opportunities or risks that emerge in a cyber context. Therefore, establishing a dedicated office or personnel whose primary focus is diplomatic engagement on cyber issues should be an integral component of a country's foreign policy.

Given the slow pace of the economic recovery, many countries are pursuing new international economic policies enshrined in trade agreements as a means to accelerate growth and create market opportunities. Yet, these economic initiatives are becoming venues where national security concerns are being negotiated, sub-rosa. For example, the Trans-Pacific Partnership (TPP) agreement was reached on 5 October 2015. The agreement's objective is to enhance trade and investment among TPP partner countries, promote innovation, economic growth and development, and support the creation and retention of jobs. It took five years to reach this agreement, in part because of cyber issues. Partner countries could not agree on key issues, including data protection and privacy requirements (e.g., intellectual property protection), data localization desires, and content restrictions.

The United States and the European Union are negotiating a Transatlantic Trade and Investment Partnership (TTIP), which is a similar agreement to the TPP. This agreement seeks to increase market access, eliminate unnecessary regulatory hurdles, establish rules to govern the entangled commercial relationships between the two regions, create jobs, and promote GDP growth.[76] Two of the core issues that are delaying this negotiation are data protection and privacy. For the past decade, Europe and the United States have agreed to common protection standards for the transfer and storage of all personal data, which moves and/or resides between the European Union and the United States.[77] However, the leaked documents by Edward Snowden exposed the United States government's intelligence services' collection activities on other governments and citizens, leading to a breakdown of trust among and between governments. As a result, many European countries are demanding the establishment of mutual state-level privacy standards, encryption rules, and legal frameworks, in order to keep pace with rapidly advancing technology and also hold states accountable for adequate protection of the data. Additionally, a recent Court of Justice of the European Union ruling has negated the long-standing agreement of "Safe Harbor" data protection standards between the European Union and the United States. The Safe Harbor executive decision had

At a fundamental level, cyber diplomacy seeks to find mutually acceptable solutions to common challenges.

allowed United States companies to self-certify to provide "adequate protection" for European users' data in compliance with the European data protection directive and with fundamental European rights, such as privacy. While negotiations are ongoing to update Safe Harbor, no time frame has been provided for completion, further complicating TTIP negotiations.[78] At present, the American Chamber of Commerce to the European Union estimates that reversing Safe Harbor could cost the European Union up to 1.3 percent of GDP.[79]

Another regionally based free trade agreement, the Regional Comprehensive Economic Partnership (RCEP) is currently under negotiation among ASEAN member states, China, India, Japan, Korea, Australia, and New Zealand. The sixteen participating RCEP countries account for almost half of the world's population, nearly 30 percent of global GDP, and over one quarter of the world exports. The goal of the RCEP is to lower trade barriers, promote economic and technical cooperation, protect intellectual property, encourage competition, facilitate dispute settlement, and improve market access for exporters of goods and services. As part of these negotiations, some countries are seeking to include mechanisms that protect their data, asserting a right to data sovereignty for national security purposes.[80]

There is also an entire series of negotiations underway in the security arena, focusing upon technologies. For example, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, which has forty-one signatories including the United States, United Kingdom, Russia, and most European Union states, recently agreed to curb the sale of Internet "communications surveillance systems" and "intrusion software" that are specially designed or modified to avoid detection by monitoring tools, or to defeat protective countermeasures.[81] States have different concerns on the dual-purpose applications of these technologies. For instance, a vulnerability assessment tool often uses zero day exploitations to discover networked vulnerabilities. These same techniques can be used as weapons. Therefore, bringing these technologies under export control regimes reflects the belief that advanced technologies may defeat countries' national defenses and present a national security risk.

Other diplomatic negotiations and discussions are ongoing that seek to establish a common understanding and/or rules to increase stability and security in the global ICT environment. This includes strengthening cooperative mechanisms to address ICT security incidents and address ICT infrastructure-related requests (e.g., illegal activity emitting from a country due to a bot-net infection). Diplomacy is also being used to define what type of cyber activities should and should not be permitted (e.g., standards for responsible state behavior), commonly referred to as *cyber norms of behavior*. For example, the United Nations GGE recently highlighted the global nature of the ICT environment, existing and potential threats in the sphere of information security, and possible cooperative measures to address those threats. The GGE found that adherence to international law, particularly UN Charter obligations, provides an essential framework for states' ICT use. They agreed to pursue a framework for cyber norms, rules or principles for responsible state behavior, and confidence-building measures (CBMs).[82] Among the CBMs, the GGE agreed to strengthen cooperative mechanisms between relevant state agencies in order to address ICT security incidents and develop additional technical, legal, and diplomatic mechanisms to address ICT infrastructure-related

requests (e.g., establish a CSIRT or other official organization to fulfill such roles). Most recently, United States President Barack Obama and Chinese President Xi Jinping agreed (in principle) to follow the GGE recommendations and adhere to UN-established norms of online behavior; especially those governing the use of cyber attacks to harm the other's critical infrastructure during peacetime.[83]

Building upon some of the common themes from the GGE, the leaders of Brazil, Russian, India, China, and South Africa (BRICS) agreed to cooperate with each other in order to address common ICT security challenges. They agreed to share information and best practices relating to the security of ICT use, coordinate against cyber crime, establish a POC network in member-states, and establish intra-BRICS cooperation using the existing CSIRTs. They also urged the international community to focus its efforts on CBMs, capacity building, the non-use of force, and the prevention of ICT enabled conflicts.[84] Moreover, in January 2015, the SCO introduced a revised international code of conduct for information security to the UNGA, which sought to identify the rights and responsibilities of states in the information space, promote constructive and responsive behavior, and enhance cooperation to address mutual ICT threats.[85] The SCO revised the 2011 Code of Conduct language with language from the 2012 and 2013 GGE reports, in order to broaden appeal for the Code of Conduct among G-77 members.

Cyber security is entangled in all components of foreign policy and trade.

Other international venues co-mingle economic, development, and security topics as they pursue specific goals. The ITU, for example, carries out regular international discussions on the policy, technology, and regulatory environment of ICT and the Internet during four of its global meetings: the World Summit on the Information Society (WSIS), the World Conference on International Telecommunications (WCIT), the World Telecommunication Development Conference (WTDC), and the World Telecommunications Standardization Assembly (WTSA).[86] In addition, the OAS and the IDB have joined forces to work with their member states to systematically address cyber security as part of three issue areas: (1) development that is both socially inclusive and environmentally sustainable; (2) ICT as a tool to generate income and employment, provide access to businesses and information, enable e-learning, and facilitate government activities; and (3) security of their core infrastructures and citizen facing services.[87]

Clearly, cyber security issues are emerging across a wide variety of diplomatic venues. Cyber security is not only a security problem; it is a fundamental element of trade, foreign and economic policy, and a country's future economic growth potential. Key components of a country's ability to effectively engage diplomatically on cyber-related issues include the establishment of a dedicated and trained cadre of personnel, the development of specific organizational structures, and the allocation of funding devoted to international discussions and negotiations on issues pertaining to cyber security. For example, Israel and the Czech Republic have placed cyber attachés in their embassies in key cities, to include Washington DC and Brussels.[88]

Additionally, the United States conducted a one-week training cyber awareness program for diplomatic personnel assigned to Asia.[89] Developing this cadre of personnel is increasingly essential for a country to realize its future foreign policy, economic policy, trade, and economic growth goals.

Elements of a sound diplomatic cyber security engagement capability should include:

Statement:

A. The announced identification of cyber security as an essential element of foreign policy and national security (e.g. Official discussions typically involving high-level political and military leaders in bilateral and multilateral discussions);

B. The announced identification of ICT and cyber security as an essential element of international economic policy, negotiations, trade, and commerce;

Organization:

A. The establishment of dedicated and trained personnel in the country's foreign office or equivalent organization whose primary mission includes active engagement internationally in cyber security diplomacy;

B. A demonstrated consistency between the numbers and ranks of dedicated foreign cyber diplomatic personnel and the announced commitment of a country to engage in cyber security diplomacy as a top tier issue of national importance;

Resources:

A. The identification of the financial and human resources requested and allocated for cyber diplomatic engagement;

Implementation:

A. Demonstrated participation in defining, signing, and enforcing international, multi-national, regional and/or bilateral agreements pursuing mutually acceptable solutions to common challenges; and

B. Demonstrated evidence of efforts to influence international trade and commerce negotiations that pertain to the use of ICT or the internationally, regionally, and/or nationally shared aspects of cyber infrastructure, critical services, and technologies.

Initial findings in this essential element are based upon a review of whether a country has explicitly designated or established a governmental office or charged individuals with diplomatic responsibilities that include both the economic and security aspects of cyber issues. The CRI 2.0 draws upon primary and secondary sources to determine whether and to what degree governmental office(s) or individuals participate in and influence international negotiations on issues pertaining to cyber security. Updates to this essential element will monitor, track, and evaluate substantive and notable developments.

7. DEFENSE AND CRISIS RESPONSE

The seventh and final element of cyber readiness is the ability of a country's national armed forces and/or related defense agency to de-

fend the country from threats emanating from cyberspace. Countries interested in this type of capability are directing their defense forces to establish capacity or expertise to respond to cyber threats that rise to the level of nationally critical "cybered" conflicts.[90]

Countries are becoming more connected and Internet-dependent that in turn is making them more vulnerable to disruptive and destructive cyber activities. Most countries' defensive postures are weak in the face of sophisticated cyber attacks. The globally connected nature of modern competitions and conflicts encourage cyber-enabled adversaries to move laterally across national systems and target a country's commercial and non-state organizations. For example, in August 2012, Saudi Aramco suffered a targeted attack that used malicious software to destroy data and damage nearly seventy five percent of the company's IT infrastructure.[91] Corporate officials claimed that the incident was intended to affect oil production. A few months later, in March 2013, multiple financial institutions in South Korea, including Shinhan Bank—the country's fourth largest bank—suffered damages from malware similar to those used against Saudi Aramco. The bank's e-services were disrupted and data was destroyed. The economic damages from this incident were estimated to have reached approximately $800 billion dollars.[92] In December 2014, hackers successfully manipulated and disrupted the control systems at a German Steel Mill, causing its blast furnace to shut down improperly, which resulted in significant damages.[93] The same year, Sony pictures fell victim to a cyber attack where unreleased motion pictures were illegally copied, corporate emails were stolen and then leaked, and financial documents were exposed. Sensitive data on tens of thousands of Sony employees were copied, and nearly 80 percent of the company's IT assets were destroyed, from data to hardware, by virulent malware.[94]

Countries must be prepared to defend their connected and networked interests for current and future conflicts. The speed and reach of the Internet helps connect all aspects of society and provides easy access to military-grade cyber weapons, giving an asymmetric advantage to many. Indeed, the diversity of malicious actors including political activists, criminals, terrorists, state and non-state actors—all with differing motives underscores the need to prepare for worst-case scenarios. At present, more than sixty countries have developed capabilities for cyber espionage and attack, while also demonstrating considerable interest in acquiring or developing defensive and pre-emptive offensive capabilities.[95] Additionally, countries have started to devise different strategies and tools to upgrade their national level cyber defenses. Most governments have instinctively looked to increase the existing defensive ca-

Disruptive and destructive cyber activities requires a credible cyber defense.

pabilities of their security agencies that already are capable of operating in, through, and as enabled by cyberspace outside their national borders (i.e. the defense organization or intelligence services). Others have sought to place these capabilities in security organizations not directly located within their military structure.[96]

For instance, in 2010 the United States established a dedicated military unit—the United States Cyber Command—to defend against cyber threats to military infrastructure. Its mission was expanded in 2015 when the Department of Defense's (DoD) published its second Cyber Strategy to guide the development of DoD cyber forces (under the command and control of United States Cyber Command) and to strengthen its cyber defenses and cyber deterrence posture. This new strategy highlights the need to be "prepared to defend the United States homeland and United States vital interests from disruptive or destructive cyber attacks of significant consequence," and to build, maintain, and use viable cyber options to control conflict escalation and shape the combat environment at all stages.[97]

Similarly, in December 2014, the Russian Federation released its new Military Doctrine that highlights Russia's development of cyber warfare capabilities for both offensive and defensive purposes as well as "non-nuclear deterrence."[98] Russia's 2011 Ministry of Defense White Paper, "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," parallels aspects of the Russian Defense Doctrine, but also explicitly includes public opinion and the need to keep the media abreast of evolving conflict situations for de-escalation purposes.[99] According to the Russian media, Russia's leadership plans to release a new Information Security Doctrine in 2016, which allegedly will propose to develop forces for information warfare and information systems for strategic deterrence and the prevention of conflicts.[100]

The Republic of South Korea (ROK) and Brazil have also established similar military organizations aimed at securing offensive, defensive, and response capabilities as well as ensuring complete victory in cyber warfare.[101] South Korea has been expanding its cyber capabilities and is reportedly training over four hundred new cyber troops for its ROK Defense Cyber Command, bringing the total to around one thousand.[102]

Additionally, while the People's Republic of China (PRC) has not publicly issued any formal strategic doctrine for cyber or information military applications, it has published Military Strategic Guidelines that provides direction for defense policy.[103] The PRC's 2013 White Paper: the *Diversified Employment of China's Armed Forces* and the 2014 "Opinion on Further Strengthening Information Security Work," stress the development of defensive cyber capabilities. The documents emphasize that the People's Liberation Army (PLA) will not attack unless attacked, but if attacked, will counterattack in cyberspace.[104]

A cyber defense agency need not be a uniformed agency within the nation's military. National police and intelligence forces can be the loci of a government's central capacity to defend in cyberspace, although the armed forces will also need to be modernized and cyber ready for more traditional conflicts. For example, Iceland has concentrated its cyber responses outside its armed forces. In the past, Icelandic cyber security responsibilities were informally divided among the Ministry of the

Interior, the Post and Telecom Administration, the Data Protection Authority, and the Icelandic Police. However, in 2015 Iceland centralized all of its cyber capabilities under the National Commissioner of the Icelandic Police.[105] Iceland's June 2015 national cyber strategy also highlights the integral role of the NATO alliance to Iceland's cyber defense.[106]

Finally, while Israel does not presently have a formalized "cyber command," its cyber security capabilities exist and are dispersed throughout the Israeli Defense Force (IDF) and the Military Intelligence Directorate. The Military Intelligence Directorate handles offensive capabilities, while the services deal with protection. Shin Bet, Israel's internal security service, is responsible for defending government systems and critical national infrastructure, and the National Cybernetic Taskforce secures critical networks and private industry against hacking and espionage.[107] This may change, however, because in June 2015, Lt. Gen. Gadi Eisenkot, commander of the Israeli Army, declared his intent to establish a new IDF corps—on par with the Navy and Air Force—responsible for all cyber activity. Should the defense minister approve the new corps, the new cyber IDF would be operational within two years. Once operational, the new Cyber Command will integrate defensive capabilities currently provided by the IDF with offensive and intelligence capacity performed by Unit 8200 and other military intelligence communities.[108] This aligns with the new IDF five-year plan, "Gideon," which was published in August 2015. "Gideon" specifically calls for increased initiatives to fend off cyber attacks and other asymmetric threats, which may emanate from non-state and terrorist groups in the region.[109]

A cyber defense capability is necessary for a country to ensure its national and economic security. As countries become more reliant on the Internet and ICT systems, the more vulnerable they will become to "low level" cyber threats and asymmetric activity. Countries are faced with a Catch-22, greater ICT uptake is essential for growth, but the more connected a country becomes the more risks they incur. Opting out of the Internet economy is no longer an option. Countries must be prepared to defend themselves in cyberspace. If a country is unable to defend itself, it is not cyber ready.

Elements of a country's commitment to develop and deploy dedicated national defense units with cyber defense capabilities/responsibilities may include:

Statement:

A. The publication of national statements that assign an organization the national cyber defense mission as a top tier mission;

B. The establishment of policies for the cyber defense organization to respond to cyber threats;

C. The articulation of national statements that direct the cyber defense organization to develop capacity to respond to threats within or outside the sovereign territory;

Organization:

A. The establishment of a national-level organization, within the military, whose primary mission is the cyber defense of the nation;

B. The establishment of a national-level organization, not within the military, whose primary mission is the cyber defense of the nation;

Resources:

A. The identification of financial and human resources requested and allocated for the organization, within the military, whose mission explicitly includes the cyber defense of the nation;

B. The identification of the financial and human resources requested and allocated for the organization, not within the military, whose mission explicitly includes the cyber defense of the nation;

Implementation:

A. Evidence of conducted government-level exercises that demonstrate national cyber defense readiness;

B. Evidence of conducted national-level exercises involving affected commercial entities that demonstrate national cyber defense readiness;

C. Evidence of conducted exercises with international partners (e.g. NATO mutual defense or APCERT Drill) that demonstrate cooperation through information exchange and assistance;

D. The establishment of standards for responsible state behavior in cyberspace and identification of thresholds that permit engagement for cyber defense; and

E. The establishment of rapid assistance mechanisms (separable from CERTs or equivalents) for the government or specific industries in case of major cyber incidents.

Initial findings in this essential element are based upon a review of whether a country has officially declared to establish defense forces whose top-level mission includes cyber defense of the nation. The CRI 2.0 draws on primary and secondary sources to determine the level of operational maturity. Updates to this essential element will monitor, track, and evaluate substantive and notable developments.

CONCLUSION

No country is cyber ready.

The threats to our networked systems and infrastructures are real and growing and impose costs in economic terms to countries and society. Economic and national security agendas must align to bring transparency to cyber insecurity. Showing this vital association may spark national and global interest in addressing this economic erosion. The CRI 2.0's comprehensive, comparative, experience-based methodology provides a blueprint to evaluate any country's maturity and commitment to securing their national cyber infrastructure and services upon which their digital future and growth depend.

The CRI 2.0 blueprint identifies over seventy unique data indicators across seven essential elements: national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response. These indicators and essential elements provide a framework for a country to develop a stronger

security posture that can defend against GDP erosion. In effect, the CRI 2.0 challenges the conventional wisdom that cyber security is predominately a national security issue. The CRI 2.0 can demonstrate how national security is closely intertwined with Internet connectivity and rapid adoption of ICT which, when secure, can lead to economic growth and prosperity.

Instead of simply studying the problem, the CRI 2.0 offers a framework for a country to evaluate the strength of its ability to prevent economic erosion from cyber insecurity. The CRI 2.0 will be updated periodically adding evaluation criteria without losing comparative validity with any prior assessments. In that way, the CRI 2.0 will demonstrate countries' progress and evolution toward securing the cyber infrastructure and services upon which their digital future and growth depend.

No country can afford cyber insecurity and the losses it incurs. The CRI 2.0 data and methodology can help national leaders chart a path to a safer, more resilient economy in a deeply cybered, competitive, and conflict-prone world.

For more information or to provide data to the CRI 2.0 methodology, please contact:

CyberReadinessIndex2.0@potomacinstitute.org

BIBLIOGRAPHY

1. The Cyber Readiness Index 2.0 builds on the previous Cyber Readiness Index 1.0, which provided a methodological framework for assessing cyber readiness across five essential elements, namely: cyber national strategy, incident response, e-crime and legal capacity, information sharing, and cyber research and development. The Cyber Readiness Index 1.0 applied this methodology to an initial set of thirty-five countries. For more information on Cyber Readiness Index 1.0, see: Melissa Hathaway, "Cyber Readiness Index 1.0," *Hathaway Global Strategies LLC* (2013), *http://belfercenter.ksg.harvard.edu/files/cyber-readiness-index-1point0.pdf*.

2. The Internet-infrastructure entanglement is the interdependence on Internet connectivity for the delivery of key services including water, electricity, transportation, communications, health, etc. For more on the Internet-infrastructure entanglement, see: Melissa Hathaway, "Connected Choices: How the Internet Is Challenging Sovereign Decisions," American Foreign Policy Interests 36, no. 5 (November 2014): 301.

3. Examples of ICT enabled economic strategies being pursed around the world include: Europe's *Digital Single Market*; India's *Digital India (ID)*; China's *Internet Plus (+)*; and the ITU *Connect 2020.*

4. State Council of China, "Internet Plus," *Guo Fa* 40 (2015). Translated by U.S. State Department.

5. Government of India, "Programme Pillars," *Digital India: Power to Empower, http://www.digitalindia.gov.in/content/programme-pillars*.

6. European Commission, "Digital Single Market: Bringing down the barriers to unlock online opportunities," *http://ec.europa.eu/priorities/digital-single-market/*.

7. Melissa Hathaway and Francesca Spidalieri, "Sustainable and Secure Development: A Framework for Resilient Connected Societies," in *Observatory of Cyber Security in Latin America and the Caribbean* (forthcoming December 2015 Organization of American States publication).

8. World Bank, "Overview," *Information & Communication Technologies Program,* last modified 2 October 2014,*http://worldbank.org/en/topic/ict/overview*.

9. David Dean et al., "The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy," *Boston Consulting Group report* (January 2012): 2.

10. Peter C. Evans and Marco Annunziata, "Industrial Internet: Pushing the Boundaries of Minds and Machines," *General Electric* (26 November 2012): 13.

11. Melissa Hathaway, "Cyber Readiness Index 2.0 & Lessons Learned in the Design of national Cyber Security Strategies," (presentation at the OAS-IDB Regional Workshop on Cyber Security Policies, Washington D.C., 23 October 2014).

12. Frontier Economics London, *Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report commissioned by Business Action to Counterfeiting and Piracy*, (London, Frontier Economics Ltd, 2011): 47.

13. The National Bureau of Asian Research, "The IP Commission Report: The report of the commission on the theft of American intellectual property," *National Bureau of Asian Research* (May 2013).

14. Melissa Hathaway, "Connected Choices: How the Internet Is Challenging Sovereign Decisions," *American Foreign Policy Interests* 36, no. 5 (November 2014): 301.

15. Harvey Poppel is credited with inventing Harvey Balls in the 1970s while working at Booz Allen Hamilton as a consultant.

16. Based on 2013 World Bank GDP rankings.

17. OECD, *OECD Digital Economy Outlook 2015* (Paris, France: OECD Publishing, 2015), *http://dx.doi.org/10.1787/9789264232440-en*.

18. Melissa Hathaway, "Transparency, Trust, and Our Internet," (presentation at GTEC Conference, Ottawa, Canada, 20 October 2015).

19. ICT infrastructure uptake includes fixed and mobile (voice and data) market segments—both subscriptions and household data access—and investment in and revenues by the telecom sector.

20. A competent authority is any person or organization that has the legally delegated or invested authority, capacity, or power to perform a designated function.

21. International Telecommunications Union, "National Strategies," *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx*.

22. The terms CSIRT and CERT refer to a team of IT security experts designated to respond to computer security incidents. Both terms are used interchangeably, with CSIRT being the more precise term.

23. The International Telecommunications Union, "CIRT Programme," *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx*.

24. John Haller, Samuel Merrell, Matthew Butkovic, and Bradford Willke, *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0* (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2011), *http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9999*.

25. Olaf Kruidhof, "Evolution of National and Corporate CERTs – Trust, the Key Factor," in *Best Practices in Computer Network Defense: Incident Detection and Response*, ed. Melissa E. Hathaway, (Amsterdam: NATO Science for Peace and Security Series, IOS Press, February 2014).

26. Singapore Computer Emergency Response Team, "FAQs," *https://www.csa.gov.sg/singcert/about-us/faqs*.

27. Ministério das Comunicações, "Portaria Interministerial N 147, de 31 de Maio de 1995," *http://cgi.br/portarias/numero/147*.

28. *cert.br*, "About *CERT.br*," *http://www.cert.br/about/*.

29. "Documents," APCERT. *APCERT.org*, 13 October 2015. *http://www.apcert.org/documents/index.html*.

30. "Asia Pacific Computer Emergency Response Team Operational Framework" APCERT. *APCERT.org*, 13 October 2015. *http://www.apcert.org/documents/pdf/OPFW(26Mar2013).pdf*.

31. Melissa Hathaway, "Best Practices in Computer Network Defense: Incident Detection and Response," Global Cyber Security Center (September 2013): 12.

32. Ingvar Hellquist (Colonel retd.), Senior Advisor and Lars Nicander, Director, Center for Asymmetric Threat Studies, Swedish Defence University, "CATS Course and Cyber Exercise," (interview by Melissa Hathaway in Stockholm, Sweden, 17 October 2012) and Swedish National Defence College, "CATS Newsletter," *CATS Center for Asymmetric Threat Studies* (Spring 2013).

33. Dusan Navratil, Director Czech Republic National Security Authority and Robert Kahofer, Special Assistant, "Cyber Czech 2015 - National Technical Cyber Security Exercise," (interview by Melissa Hathaway in Washington DC, October 2015).

34. "South Korea says Nuclear Worm is nothing to worry about," *TheRegister.co.uk*, 30 December 2014, *http://www.theregister.co.uk/2014/12/30/south_korea_says_nuclear_worm_is_nothing_to_worry_about/* and "Activists Hack KNHP's computer systems," World Nuclear News, 22 December 2014, *http://www.world-nuclear-news.org/C-Activists-hack-KHNPs-computer-systems-2212141.html*.

35. Department of Homeland Security, "Cyber Storm: Securing Cyber Space," *http://www.dhs.gov/cyber-storm-securing-cyber-space*.

36. European Commission, "Cyber Strategy of the European Union: An Open, Safe, and Secure Cyberspace," *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,* (July 2013): 7 and European Union Agency for Network and Information Security, "Cyber Europe," *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe*.

37. Doug Drinkwater, "Hundreds of companies face two thousand cyber-attacks in EU exercise," SC Magazine, 31 October 2014 in ENISA, "ENISA Cyber Europe 2014: Media Coverage," *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/cyber-europe-2014-media-coverage*.

38. European Defense Agency, "Complex Cyber Crisis Management Exercise in Vienna," 16 September 2015, *https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/09/16/complex-cyber-crisis-management-exercise-in-vienna* and NATO, "Largest ever NATO cyber defence exercise gets underway," 21 November 2014, *http://www.nato.int/cps/en/natohq/news_114902.htm?selectedLocale=en*.

39. Katie Bo Williams, "US, UK to test finance sector cybersecurity this month," The Hill, 2 November 2015, *http://thehill.com/policy/cybersecurity/258827-us-uk-to-test-finance-sector-cybersecurity-this-month*.

40. CNCERT/CC, "2nd China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response was held in Korea," *www.cert.org.cn/publish/english/55/2014/20140916145739295996084/20140916145739295996084_.html*.

41. Carnegie Mellon University, "List of National CSIRTs," CERT Division, *http://www.cert.org/incident-management/national-csirts/national-csirts.cfm*.

42. European Network and Information Security Agency (ENISA), "ENISA- CERT Inventory: Inventory of CERT teams and activities in Europe," ENISA Version 2.16 (June 2014), *http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe*.

43. Forum of Incident Response and Security Teams (FIRST), "FIRST Members," *http://www.first.org/members/teams*.

44. Council of Europe, *Convention on Cybercrime* (23 November 2001) and Shanghai Cooperation Organisation, *Cooperation in the Field of Information Security,* 61 plenary meeting (16 June 2009).

45. *Ibid*.

46. Shanghai Cooperation Organisation, *Cooperation in the Field of Information Security,* 61 plenary meeting (16 June 2009), *https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf*.

47. Judge Stein Schjolberg and Amanda M. Hubbard, "Harmonizing National Legal Approaches on Cybercrime," International Telecommunication Union (1 July 2005): 6.

48. The twenty countries that signed the GGE report, include: Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Korea, Russia, Spain, the UK, and the USA. See: United Nations, Report of the Group of Government Experts On Development in the Field of Information and Telecommunications In the Context of International Security, A/65/201 and A/68/98 (26 June 2015).

49. Ernesto U. Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement, and Research (Dordrecht, The Netherlands: Springer, 2004): 50.

50. Advanced Centre for Research, Development and Training in Cyber Laws and Forensics, "Academic Programs," *National Law School of India University, https://www.nls.ac.in/index.php?option=com_content&view=article&id=502&Itemid=32*.

51. INTERPOL, "The INTERPOL Global Complex for Innovation," accessed 17 September 2015, *http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation*.

52. Madan M. Obero, "Dark Web and Crypto-Currency," (presentation at Cyber 360: A Synergia Conclave, Bangalore, India, 30 September 2015).

53. A bot is a malicious form of software that could use your computer to send spam, host a phishing site, or steal your

identity by monitoring your keystrokes. Infected computers are then controlled by third parties and can be used for cyber attacks. For more information, see: Melissa Hathaway and John Savage, "Stewardship of Cyberspace: Duties of Internet Service Providers," Cyber Dialogue 2012 (March 2012).

54. Alastair Stevenson, "Botnets infecting 18 systems per second, warns FBI," *V3.cok.uk*, 16 July 2014, *http://www.v3.co.uk/v3-uk/news/2355596/botnets-infecting-18-systems-per-second-warns-fbi*.

55. Bell Canada et all, "The Dark Space Project," *Security Telecommunications Advisory Committee* (2011): 13, *https://citizenlab.org/cybernorms2012/cybersecurityfindings.pdf*.

56. Yurie Ito, "Cyber Clean Center," (remote interview with Cyber Readiness Index team, Washington DC, 10 November 2015).

57. Ministry of Internal Affairs and Communications and Ministry of Economy Trade and Industry, "What is the Cyber Clean Center," *Cyber Clean Center, https://www.telecom-isac.jp/ccc/en_index.html* and Michael M. Losavio, J. Eagle Shutt, and Deborah Wilson Keeling, "Changing the Game: Social and Justice Models for Enhanced Cyber Security," in Tarek Saadawi, Louis H Jordan Jr., and Vincent Boudreau, Cyber Infrastructure Protection Volume II (U.S. Army War College, Strategic Studies, 2013): 101.

58. Telecom-ISAC Japan, "Chairman's Message," 12 May 2011, *https://www.telecom-isac.jp/english/index.html*.

59. Australian Internet Security Initiative (AISI), "Overview of the Australian Internet Security Initiative," *http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative*.

60. McAfee, "McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies," June 9, 2014, *http://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx* and The National Bureau of Asian Research, IP Commission Report: The report of the commission on the theft of American intellectual property," National Bureau of Asian Research (May 2013).

61. Melissa Hathaway, "Why Successful Partnerships are Critical for Promoting Cybersecurity," The New New Internet, 7 May 2010.

62. Netherlands Ministry of Security and Justice, "National Cyber Security Centre (NCSC)," *https://www.ncsc.nl/english*.

63. In February 2007, the UK National Infrastructure Security Coordination Center merged with the National Security Advice Center (NSAC) for form the Centre for the Protection of National Infrastructure (CPNI). For more on CPNI, see: Center for Protection of National Infrastructure, *http://www.cpni.gov.uk*.

64. Information-technology Promotion Agency (IPA), Japan IT Security Center, *Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) Annual Activity Report FY2012*, (April 2013).

65. Financial Services-Information Sharing and Analysis Center, "Overview of the

FS-ISAC," accessed 17 September 2015, *https://www.fsisac.com/sites/default/files/FS-ISAC_Overview_2011_05_09.pdf*.

66. National Cyber-Forensics & Training Alliance, "Become a NCFTA Partner," *https://www.ncfta.net/become-ncft-partner.aspx*.

67. Raphael Mandarino, "MT2: Private Public Partnership," Institucional Security Cabinet, Department of Information Security and Communications, Office of the President, (presentation at 1st INTERPOL Security Conference, Hong Kong, 15-17 September 2010).

68. National Institute for Standards and Technology, "National Vulnerability Database," *https://nvd.nist.gov*.

69. The UK and Brazil have mechanisms in place to declassify (write-for-release) intelligence information and share it with their critical sectors, much better than the US does.

70. European Commission, "ICT Research & Innovation," *Horizon 2020: The EU Framework Programme for Research and Innovation, http://ec.europa.eu/programmes/horizon2020/en/area/ict-research-innovation*.

71. For more on the Networking and Information Technology Research and Development Program (NITRD) and its research areas, see: *www.nitrd.gov/Index.aspx* and NITRD, "The Networking and Information Technology and Research Development Program," *Supplement to the President's Budget FY 2016* (February 2015), *https://www.whitehouse.gov/sites/default/files/microsites/ostp/fy2016nitrdsupplement-final.pdf*.

72. Consulate General of Israel in New York, "Cabinet approves tax break for National Cyber Park," Consulate General of Israel in New York, 7 June 2014, *http://embassies.gov.il/wellington/NewsAndEvents/Pages/Cabinet-approves-tax-break-for-National-Cyber-Park-6-Jul-2014.aspx*.

73. Ciência Sem Fronteiras, "FAQ", *http://www.cienciasemfronteiras.gov.br/web/csf-eng/faqEGTI_2013*-2105_v1-3, Coordination for the Improvement of Higher Education Personnel (CAPES), "Coordination for the Improvement of Higher Education Personnel (CAPES)", *http://www.iie.org/Programs/CAPES*, and CNPq, "Programas Institucionais de Iniciação Científica e Tecnológica," *http://www.cnpq.br/web/guest/piict*.

74. "Cyber Security," *The Hague Security Delta*, *https://www.thehaguesecuritydelta.com/cyber-security*.

75. Zach Cutler, "5 Growing Cyber-Security Epicenters Around the World," *Entrepreneur*, 3 September 2015, *http://www.entrepreneur.com/article/250024*.

76. European Commission, "About TTIP," *Trade, http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/*.

77. "Welcome to the U.S.-EU Safe Harbor," *http://www.export.gov/safeharbor/eu/eg_main_018365.asp*.

78. Court of Justice of the European Union, "The Court of Justice declares that

the Commission's US Safe Harbour Decision is invalid," *Press Release* 117/15 (6 October 2015), *http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf*.

79. American Chamber of Commerce to the European Union, "EU Courts of Justice's decision in the Schrems case could disrupt transatlantic business, hurt the EU economy and jeapordise a Digital Single Market," Press Release, 6 October 2015, *http://www.amchameu.eu/sites/default/files/press_releases/press_-_ecj_decision_on_schrems_will_disrupt_transatlantic_business.pdf*.

80. Hathaway, "Connected Choices: How the Internet Is Challenging Sovereign Decisions," 302 and Arun Mohan Sukmar, "The New Great Game in Asia," *The Hindu,* 25 August 2015, accessed September 16, 2015, *http://www.thehindu.com/opinion/op-ed/arun-mohan-sukumar-column-the-new-great-game-in-asia/article7575755.ece*.

81. "Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies" last updated 16 September 2015, *http://www.wassenaar.org/index.html*.

82. United Nations, *Report of the Group of Government Experts On Development in the Field of Information and Telecommunications In the Context of International Security*, A/65/201 and A/68/98 (26 June 2015).

83. The White House Office of the Press Secretary, "FACT SHEET: President Xi Jinping's State Visit to the United States," 25 September 2015, *https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states*.

84. University of Toronto, "VII: BRICS Summit 2015 Ufa Declaration," *BRICS Information Centre,* 9 July 2015, *http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html*.

85. United Nations, General Assembly, "Letter dated 9 January 2015 from Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General," Developments in the field of information and telecommunications in the context of international security, A/69/723 (13 January 2015), *http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement*.

86. Melissa Hathaway, "Discussion Paper for the Global Commission of Internet Governance," (paper presented in Stockholm Sweden, 27 May 2014).

87. Inter-American Development Bank, "IDB and OAS join efforts to promote better cybersecurity policies in Latin America and the Caribbean," 22 October 2014, *http://www.iadb.org/en/news/news-releases/2014-10-22/cybersecurity-workshop-for-latin-america,10957.html*.

88. Dusan Navratil, Director Czech Republic National Security Authority and Robert Kahofer, Special Assistant, "Cyber Czech 2015 - National Technical Cyber Security Exercise," (interview

by Melissa Hathaway in Washington DC, October 2015) and Rueuven Azar, Deputy Chief of Mission and Dr. Eviatar Matania, Head of National Cyber Bureau (interview by Melissa Hathaway in Rockville, MD, 2 June 2015).

89. Craig L. Hall, US Consulate General, Kolkata, India, (interview by Melissa Hathaway in Kolkata, India, 23 September 2015).

90. Cybered conflict differs from cyber war or cyber battle. The latter is fully technological and could, in principle, be conducted entirely within a network. It is normally a component of the former. "Cybered conflicts are those nationally significant aggressive and disruptive conflicts for which seminal events determining the outcome could not have occurred without 'cyber' (meaning networked technologies) mechanisms at critical junctures in the determining course of events." Chris Demchak, "Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World," in Securing Cyberspace: A New Domain for National Security, edited by Nicholas Burns and Jonathon Price, (Washington, DC: The Aspen Institute, 2012).

91. Christopher Bronk, "The Cyber Attack on Saudi Aramco," Survival 55 (April-May 2013) 81-96.

92. Melissa Hathaway and John Stuart, "Cyber IV Feature: Taking Control of our Cyber Future," *Georgetown Journal of International Affairs* (25 July 2014).

93. Robert M. Lee, Michael J. Assante, and Tim Conway, "German Steel Mill Cyber Attack," *Industrial Control Systems* (30 December 2014).

94. "The Reality of the Sony Pictures Breach," *TrendMicro*, 22 December 2014, *http://blog.trendmicro.com/reality-sony-pictures-breach/*, Sean Fitz-Gerald, "Everything That's Happened in the Sony Leak Scandal," *Vulture*, 22 December 2014, *http://www.vulture.com/2014/12/everything-sony-leaks-scandal.html#*, and "Sony Breach May Have Exposed Employee Healthcare, Salary Data," *Krebson Security*, 2 December 2014, *http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/*.

95. Jennifer Valentino-Devries and Danny Yadron, "Cataloging the World's Cyberforces," The Wall Street Journal, 11 October 2015, *http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710* and United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the context of International Security: Report to the Secretary General*, A/70/172 (22 July 2015), *http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172*.

96. James Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization," *UNIDIR Resource and Center for Strategic and International Studies* (2011): 3.

97. Department of Defense, "The Department of Defense Cyber Strategy," (April 2015): 7-8.

98. President of the Russian Federation, "Military Doctrine of the Russian Federation," *Russian Government* (2014)

translated by Thomas Moore, *https://www.scribd.com/doc/251695098/Russia-s-2014-Military-Doctrine*.

99. Ministry of Defense of the Russian Federation, "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space," (2011) translated by the US Department of State.

100. "The new doctrine of information security pointed out the danger of destabilization via the Internet," *Russian News*, 10 September 2015, *http://en.news-4-u.ru/the-new-doctrine-of-information-security-pointed-out-the-danger-of-destabilization-via-the-internet.html*.

101. The Brazilian Ministry of Defence has also recently instructed the Armed Forces Joint Chiefs of Staff (EMCFA) to enhance national cyber defense through the creation of a tri-service Cyber Defense Command (ComDCiber). While ComDCiber will comprise all three services, the Army will take the lead. ComDCiber will be based off of the previously established Brazilian Cyber Defense Center Nucleus (NU CDCiber) in Brasília. See eelnigo Guevara, "Brazil to stand up Cyber Defence Command," IHS Jane's Defence Weekly, 4 November 2014 and Diego Rafael Canabarro and Thiago Borne, "Brazil and the Fog of (Cyber) War," National Center for Digital Governance (2013): 5. On Korea's cyber capabilities, see : Republic of Korea, "Defense White Paper," (2014), 57, *http://www.mnd.go.kr/user/mnd_eng/upload/pblictn/PBLICTNEBOOK_20150161156164570.pdf*.

102. Zachary Keck, "South Korea Seeks Offensive Cyber Capabilities," *The Diplomat*, October 11, 2014, *http://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites/*.

103. For an overview of China's cyber strategy, see: Amy Chang, "Warring States," *The Center for New American Security*, (December 2014).

104. Information Office of the State, "White Paper: The Diversified Employmenet of China's Armed Forces," April 2013, *http://eng.mod.gov.cn/Database/WhitePapers/* and Xi Jinping, Cental Military Commission, "Opinion on Further Strengthening Military Information Security Work," partial translation from Amy Chang, "Warring States," The Center for New American Security, (December 2014): 20.

105. Director Generals of Nordic Council, "Icelandic Cyber Responsibilities," (meeting between Melissa Hathaway and Director Generals and respective delegations of the Nordic Council who are responsible for National Computer Emergency Response Teams, Stockholm, Sweden, 19 November 2014).

106. Minister of the Interior, "Icelandic National Cyber Security Strategy 2015-2026: Plan of Action," Icelandic Minister of the Interior (June 2015), *http://eng.innanrikisraduneyti.is/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf*.

107. Yaakov Katz, "Security and Defense," *The Jerusalem Post*, 8 October 2010 in James Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization," *UNIDIR Resource and Center for Strategic and International Studies* (2011), 14 and "Eye on tech exports, Israel launches cyber command," *Reuters,* 18 May 2011, *http://www.reuters.com/article/2011/05/18/us-israel-security-cyber-idUSTRE74H27H20110518*.

108. Mitch Ginsburg, "Army to establish unified cyber corps," The Times of Israel, June 16, 2015.

109. Michael Herzog, "New IDF Strategy Goes Public," The Washington Institute: Policy Watch 2479 (28 August 2015), *http://www.washingtoninstitute.org/policy-analysis/view/new-idf-strategy-goes-public*.

ABOUT THE AUTHORS

Melissa Hathaway is a leading expert in cyberspace policy and cybersecurity. She serves as a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies and is a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs. She also is a Distinguished Fellow at the Centre for International Governance Innovation in Canada and was appointed to the Global Commission for Internet Governance (Bildt Commission). She served in two Presidential administrations where she spearheaded the Cyberspace Policy Review for President Barack Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. She developed a unique methodology for evaluating and measuring the level of preparedness for certain cybersecurity risks, known as the Cyber Readiness Index. She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following website: *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html*.

Chris Demchak is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. Her research areas are digital resilience, cyber conflict, and the structures and risks of cyber space. She designed a digitized organization model known as "Atrium" that helps large enterprises respond to and accommodate surprises in their systems. She is also the author of Wars of Disruption and Resilience: Cybered Conflict, Power and National Security.

Jason Kerben is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. He also serves as senior advisor to multiple Departments and Agencies in matters related to information security and cyber security. In particular, he focuses on legal and regulatory regimes that impact an organization's mission. He develops methodologies and approaches to assess and manage cyber security risk and advises on a myriad of specific cybersecurity activities including international principles governing information and communications technologies, identity and access management, continuous diagnostics and mitigation and cyber insurance.

Jennifer McArdle is a Fellow in the Center for Revolutionary Scientific Thought at the Potomac Institute for Policy Studies. Her academic research focuses on cyber warfare, information warfare, and Asian geopolitics. She is currently a PhD candidate at King's College London in the War Studies department.

Francesca Spidalieriis a subject-matter expert at the Potomac Institute for Policy Studies' Cyber Readiness Index Project. She also serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University. Her academic research and publications have focused on cyber leadership development, cyber risk management, cyber education and awareness, and cyber security workforce development. She recently published a report, entitled "State of the States on Cybersecurity," that applies the Cyber Readiness Index 1.0 at the US state level.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org