



A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China

By Jing de Jong-Chen¹ and Bobby O'Brien

November is the “Critical Infrastructure Security and Resilience Month” in the U.S., as designated by the Department of Homeland Security (DHS). It is an appropriate time to reflect on the importance of Critical Infrastructure Protection (CIP), as well as the legislative and administrative efforts being undertaken in the U.S., E.U. and China to establish robust CIP frameworks and enforcement policies. There is a broad-scale recognition among policy makers across the globe that collaborative efforts between public and private sectors are required to develop and enforce effective CIP measures, especially as the rapid pace of technological

innovation and adoption drives digital transformation and, at the same time, increases cyber threats.

To better understand global policy approaches toward CIP, this paper will review the efforts of the U.S., E.U., and China to address critical infrastructure protection in their domains. The paper will then offer a set of proposed principles and global best practices that may aid policy makers and industry stakeholders as they consider how best to move forward in addressing CIP-related opportunities and challenges.

The U.S. Approach to CIP and the National Institute of Standards and Technology (NIST) Cybersecurity Framework

Definition of Critical Infrastructure and the Agencies Responsible for Managing CIP

The US Presidential Policy Directive 21 (“Critical Infrastructure Security and Resilience”) defines critical infrastructure as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”² The U.S. is currently working toward identifying sectors that are truly critical based on the impact they have on the public. Today it recognizes 16 critical infrastructure sectors and assigns responsibility for protecting them to specific government agencies. For example, DHS is responsible for ten of the 16 sectors.³ The Office of Infrastructure Protection (IP) within the National Protection and Programs Directorate (NPPD) is responsible for coordinating critical infrastructure protection at the national-level.⁴

In 2013, Presidential Executive Order 13636 (“Improving Critical Infrastructure Cybersecurity”) tasked the U.S. National Institute of Standards and Technology (NIST) to lead the development of a framework to minimize cybersecurity risks to critical infrastructure, seeking feedback from public and private sector stakeholders and incorporating industry best practices to the fullest extent possible.⁵ Over a one-year period, NIST managed open workshops and consultations, coordinated numerous iterations of the standard, and led active

partnership between the government and the private sector.

In 2014, NIST published the Cybersecurity Framework for Protecting Critical Infrastructure (NIST Framework), describing it as a “risk-based set of industry standards and best practices to help organizations manage cybersecurity risks.” NIST is actively working on a revision to the Framework, again convening stakeholders in open workshops and seeking feedback through consultations. Among other components, the next version of the Framework will include a strengthened approach to cyber supply chain risk management (C-SCRM) including the protection of industrial controls systems as a part of the cyber critical infrastructure.⁶

The NIST Framework consists of three parts (see “Figure 1” below):

1. Framework Core

- The Framework Core contains “a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.”

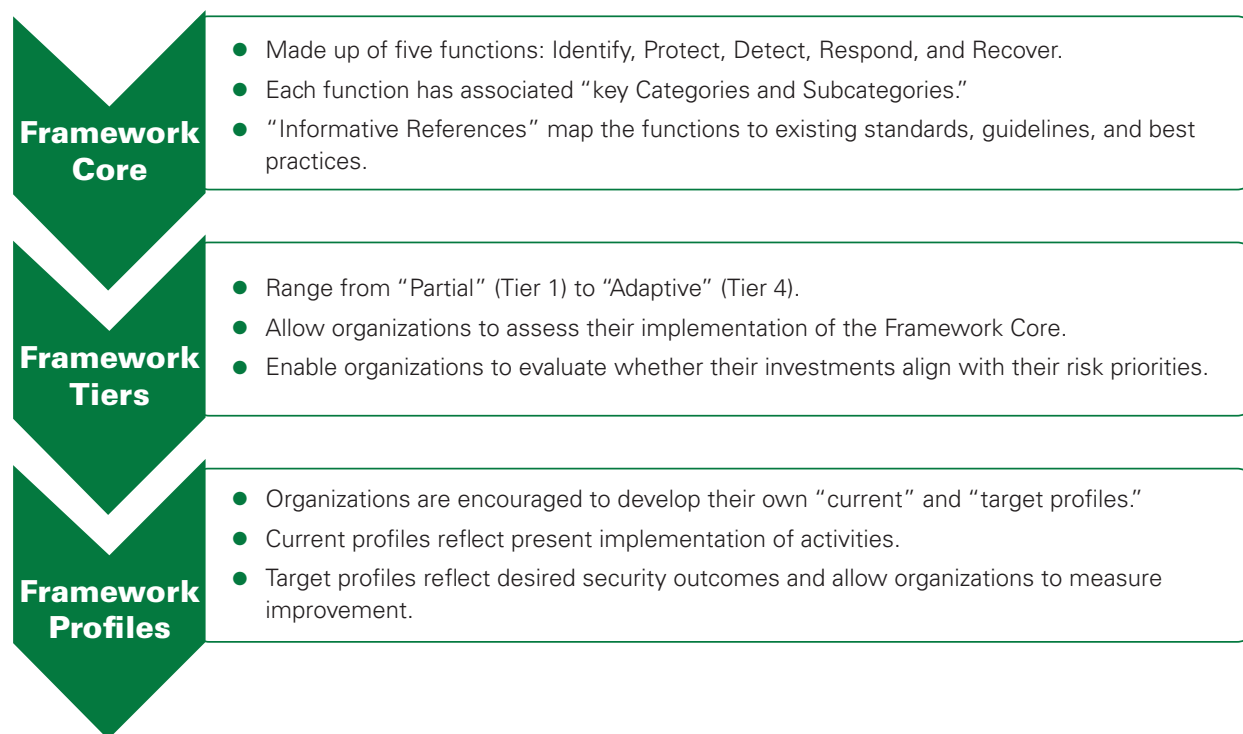
2. Framework Implementation Tiers

- The Framework Implementation Tiers enable organizations to assess their implementation of the Framework Core, allowing them to determine whether their security investments align with their risk priorities.

3. Framework Profile

- The Framework Profile provides a way for organizations to depict their current implementation of a range of security activities and compare that to their desired or target state.

Figure 1 - NIST Framework



CIP-Related Data Controls, Certification Scheme, and Adoption

The NIST Framework is designed to be flexible, scalable, industry agnostic, and technology neutral. It contains no specific restrictions on cross-border data transfer related to CIP and endorses the use of international standards and certifications for critical infrastructure protection.⁷

As a member of the Common Criteria Recognition Arrangement (CCRA), the U.S. government promotes a collaborative government protection profile development approach to encourage private sector participation and continues to accept

Common Criteria-based security certification for certain government procurement.⁸

Many organizations that are considered as critical infrastructure providers are using or aligning with the NIST Framework as a baseline for their approach to cybersecurity with adaptations made in its implementation that meet their respective security needs. The active participation of many key stakeholders, including the private sector, in the Framework’s development has led to its relatively rapid adoption by American and international organizations since the initial release in 2014.⁹

The European Union's Approach and the Network and Information Security (NIS) Directive

Definition of Critical Infrastructure and the Agencies Responsible for Managing CIP

The European Union's Network and Information Security Directive ("NIS Directive") took effect on August 8, 2016 and must be transposed into national law in E.U. member states by May 9, 2018.¹⁰ It represents the first regional-wide effort to harmonize cybersecurity and notification requirements, targeting "operators of essential services" (OESs) and "digital service providers" (DSPs).¹¹

OESs are the European equivalent of "critical infrastructure providers" in the U.S., and the NIS Directive gives E.U. member states the responsibility to identify OESs within their territory by November 9, 2018. To facilitate this process, the NIS Directive provides the following guidance in Article 5(2): "The criteria for the identification of the operators of essential services [...] shall be as follows: (a) an entity provides a service which

is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service."¹²

The NIS Directive was developed over a three-year period in response to a 2013 European Commission Proposal and "lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market." Development of the Directive was an iterative process which included public consultations and surveys, workshops with entities such as the European Network and Information Security Agency (ENISA), numerous iterations, and active partnership between the government and the private sector.¹³

The Directive's content is wide-ranging but is focused primarily on establishing cooperative mechanisms to aid regional-wide efforts at enhancing CIP, along with parameters for member-state transposition of the Directive into national law (see "Figure 2" below).



Figure 2 - NIS Directive¹⁴

The NIS Directive...

- lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;
- creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;
- creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;
- establishes security and notification requirements for operators of essential services and for digital service providers;
- lays down obligations for Member States to designate national competent authorities, single points of contact, and CSIRTs with tasks related to the security of network and information systems.

CIP-Related Data Controls, Certification Scheme and Adoption

Even though EU released its General Data Protection Regulation in 2016 to promote privacy protection¹⁵, the NIS Directive, which was released in the same year, did not include restrictions around cross-border data transfer for CIP. Regarding security certification schemes, the Directive states that "Member States shall [...] encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems."

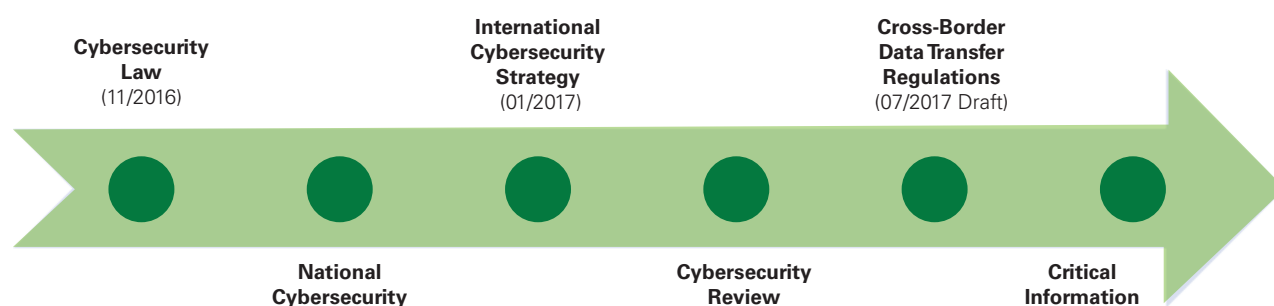
E.U. member states are expected to use the Directive as a baseline for their approach to cybersecurity (particularly as it relates to CIP), with adaptations made in its implementation that meet their unique national needs. The Directive also stresses that the "prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary E.U.-wide certification schemes building on existing schemes in the E.U. and internationally." EU member states are actively developing guidelines to drive compliance of the NIS Directive¹⁶.

China's Approach: Draft Critical Information Infrastructure Regulation and Standards

Over the past year, China's drive to protect its critical information infrastructure has led to the inclusion of Critical Information Infrastruc-

ture Protection (CIIP) in numerous government strategy documents, laws, and regulations (see "Figure 3" below).¹⁷

Figure 3 - CIIP in China (2016-2017)



As a part of the implementation of the China Cybersecurity Law, which took effect on June 1, 2017, the Cyberspace Administration of China (CAC) released a draft CIIP Regulation for public comment on July 11, 2017. It consists of eight chapters and 55 articles written, according to the regulation, "with a view to assuring the security of critical information infrastructure and in accordance with the Cybersecurity Law of China."

Definition of CII Providers and the Agency Responsible for Managing CIIP

While many governments identified the scope of critical infrastructure protection in a similar fashion, there is a subtle, but important difference in terms of how the Chinese government used the term as "critical information infrastructure protection (CIIP)" to include both traditional sectors and large-scale commercial Internet services, including

eCommerce, search and social media. The U.S. and E.U.'s definition of critical infrastructure protection (CIP) includes mostly traditional sectors and industrial systems. The US government is making an effort to narrow the scope of critical infrastructure definition to focus on the protection of the most critical public services.

The current definition of critical information infrastructure provider under the CAC draft CIIP Regulation, Article 18, includes the following:

- Government departments and organizations in the sectors/fields including energy, finance, transportation, water conservancy, health and medical care, education, social security, environmental protection, and utilities;
- Information network operators such as telecommunications networks, radio and TV

networks and the Internet, and organizations providing cloud computing, big data and other large-scale public information network services;

- Research institutions and manufacturing enterprises in the sectors/fields such as national defence, science and technology, makers of large equipment, chemical engineering, food and drugs;
- Press agencies such as radio stations, TV stations, and news agencies;
- Other key organizations.

Article 19 of the draft Regulation outlines the agencies that are responsible for CIIP in the following fashion: the Internet management agencies will work with the State Council telecommunication management agencies and public security agencies to develop guidelines for the identification of CII, and that state-owned sectors will be led by the relevant government agencies/ministries to identify CII in their respective fields.

CIIP-Related Data Controls and Operation Localization Requirements

CAC draft CIIP Regulation Articles 29 and 34 require data and operation residency. Article 29 states that “the personal information and important data collected and generated by [CII] operators during their operations within the People’s Republic of China be stored in China.” Article 34 states that “the operation of and maintenance of CII shall be carried out within China.”

While requirements keeping data storage and operation location within territorial borders may guarantee government’s access to data and operation information, in general, specific

location offers no guarantee of enhanced data or operations security. In a globalized economy, certain restrictions around data and operation will have an impact on commercial activity and the exchange of data, including as related to international banking, transportation, health care, disaster recovery, scientific research, etc. In a separate but related effort, CAC completed its third revision of the cross border data transfer policy. It is yet to be finalized. How to manage data flow and operation restrictions in a country with exponential Internet usage growth and robust international trade remains a challenge. It is important to consider the impact of such policy towards global commerce and the adoption of cutting-edge technologies by both private and public sectors to drive digital transformations worldwide.

CIIP Standards and Certification Scheme

China’s national security standards-making body, TC260, has been advancing its work on multiple standards focused on CIIP with the involvement of government, academic and industry experts. In addition, China’s Ministry of Public Security has been managing its Multilevel Protection Scheme (MLPS) compliance over the past decade. MLPS is a risk-based system that includes system classification and security certifications required for IT systems. Critical infrastructure, including government systems, are defined as “Level 3 and above” based on their potential impact on national security.

“Secure and Controllable” are used as key two requirements for security assurance in China. The same policy objective was outlined in the China Cybersecurity Law, and is used as the base for managing CIIP related technology procurement. CAC draft CIIP Regulation Articles 30-32 requires all CII operators to closely manage the security of their suppliers, including subjecting those products

or services which “may impact national security” to a security assessment by the CAC Cybersecurity Review Office. Any CIIP-related cross border data transfer will also be subject to the Cybersecurity Review, a separate but related policy issued by the CAC.

In combination, these strategies, laws, regulations, and standards comprise an ambitious and complex matrix of CIIP governance in China.

Summary

The U.S., E.U., and China each remain in the formative stages of developing their approaches to CIP. The NIST Cybersecurity Framework is an evolving document that is being updated at this moment. The NIS Directive is the precursor to associated laws being adopted in E.U. member states. China’s CIIP Regulation remains in draft form, while a draft Critical Information Infrastructure Protection Bill is expected to be unveiled in the near future.¹⁸

It is worth mentioning that there are differences between the U.S., E.U. and China in terms of the role of private sector. The U.S. and E.U. promote

the idea of private sector’s participation during the legislative process, and in response, the private sector regards the support as an obligation to provide input and expectations about the CIP policy and compliance. The Chinese government also views the increased transparency as of importance. Even though there is no formal process during the legislative process for the private sector to be involved, the Chinese government has commonly used a 30-day public comment period to collect feedback shortly before a policy is revised. Additionally, the traditional critical infrastructure operators are privately-owned in the U.S. and E.U., whereas most operators in similar CIP sectors in China are state-owned, apart from the Internet web service sector.

Regardless of the composition and geographic locations of the critical infrastructure operators and the technology providers, it is very important that government CIP policies maintain the characteristics of “flexible, scalable, industry agnostic, and technology neutral”. Figure 4, below, presents a summary view of critical infrastructure protection approaches used by the governments of the U.S., E.U., and China:

Figure 4 - Comparative Approaches to CIP in the U.S., E.U., and China

	U.S.	E.U.	China
Primary CIP Policy Drivers	Executive Order and NIST Cybersecurity Framework	NIS Directive (Law)	China Cybersecurity Law, Draft CIIP Regulation, Cross Border Data Transfer Regulation, Cybersecurity Review Regulation, MLPS
Private Sector Participation During Legislation	Yes	Yes	No
Primary Legislation Feedback Channel(s)	Workshops and Request for Information (RFI)	Public Consultations; Surveys	30-Day Public Comment Period
Risk-Based Definition of Critical Infrastructure	Yes	Yes	Yes
Data and Operation Residency Requirements	No	No	Yes
Endorsement of Global Standards	Yes	Yes	No ¹⁹

Recommendations and A Way Forward

Based on the observations of these governments' CIP legislation and regulation development, the paper recommends the following principles and best practices for governments to address the need for critical infrastructure protection, while minimizing the impact to technology innovation, adoption and global trade.²⁰

- **Promote public private partnership with a collaborative approach**

Both the public and private sectors have a common goal to ensure the safety of the public and the security of the critical infrastructure. The private sector also has extensive investment in and technology expertise regarding operating and managing global systems and networks. Partnership between the public and private sector is required to achieve the common objective of CIP. Developing the policies, programs, and capabilities for CIP requires a long-term commitment from both policy-makers

and the owners and operators of the infrastructure. A collaborative approach to develop CIP measures increases broad stakeholders' involvement to provide necessary input and allows greater readiness for compliance once measures are enforced.

A collaborative approach also increases understanding *within* organizations to deliver effective risk management and increase accountability and leadership awareness, which could lead to more informed investments. By increasing understanding *between* organizations, such as across interdependent sectors, supply chain security can be improved.

The European Commission (EC) and ENISA's work developing the NIS Directive is an example of public/private sector partnership with a collaborative approach. To optimize the impact of the Directive, the EC and ENISA organized and facilitated numerous public consultations and surveys over an extended period of time, and included discussion focused specifically on how best to partner with the private sector in protecting critical infrastructure.²¹

- **Ensure CIP measures advance security through a risk-based and outcomes-focused approach**

Risk-based approaches allow organizations with limited resources to focus their investments on the areas of security that most impact their core function. Outcome-focused approaches – approaches which identify end goals in terms of security rather than a specific implementation for achieving that end goal – allow organizations the flexibility to customize their approach in a manner that is most responsive to their unique architectures and capabilities, and enable ongoing innovation in security.

The NIST Cybersecurity Framework is a great example of a risk-based and outcome-focused approach. It is an approach to CIP which enables organizations to look inward and prioritize the risks that are potentially most impactful to them while simultaneously providing the flexibility to innovate as needed in addressing those risks rather than being required to mitigate them in a pre-prescribed manner.

- **Ensure CIP measures adopt international standards whenever possible and utilize existing best practices to the greatest extent**

Approaches to CIP are rapidly maturing as relevant governance measures around the world are being implemented. Learnings from these implementations should be used to inform updates. International standards are formulated in an inclusive, open, and collaborative manner, reflecting the expertise and input of a diverse array of stakeholders. Utilizing international standards and certifications will significantly improve efficiency for Information and Communications Technology (ICT) suppliers that engage with government customers across national borders, fostering enhanced international trade and innovation prospects. While many international standards can be used to address specific elements of CIP (such as ISO 27001 and ISO 27036), ISO/IEC 27103 ("Standing Document SD 27013 Cybersecurity and ISO and IEC Standards") specifically outlines a risk-based and outcomes-focused approach relevant for CIP.

Both the U.S. and EU outlined the endorsement of international standards in their CIP policies. Even though the draft CIIP policy issued by China proposed the usage of national standards for security assessment, TC260, China's national security standard committee, invited government,

industry, and academic experts to develop CIIP standards in support of the legislation. To develop Chinese national standards, TC260 workgroups often review internationally-developed policies, principles, best practices and standards related to its area of focus. In general, the participation of global industry in various CIP related national standard development in any region will also offer much needed technical and business expertise, minimize impact to business and increase the efficiency of compliance in a globally connected economy.

- **Promote global collaboration for CIP**

While critical infrastructure protection is important to individual countries, it is increasingly a concern for the global community. With increased cyberattacks targeting critical infrastructures such as banking and financial services, domestic and international transportation systems, the power supply, and healthcare, the availability and integrity of the data as well as the security and reliability of core Internet mechanisms must be protected by all stakeholders.

An example related to the collaborative effort to protect CIP is that associated with the development of cyber norms. The United Nations Group of Governmental Experts (UNGGE) began the work of promoting global collaboration on CIP in its groundbreaking July 2015 report, which established the following norms:

- A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical

infrastructure to provide services to the public;

- States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account the regard for sovereignty.²²

The UNGGE process produced a set of voluntary principles, but there was no consensus this year to issue a follow-on report to the 2015 version. Looking at the intensity of the cyberattacks launched by nation-states and related actors, the world may need a set of legally binding agreements to enforce the earlier norms. The private sector in the US began to voice the need for accountability towards global CIP protection and issued call to action during the RSA in 2017.²³ Much more remains to be done in this space. Principle-based global collaboration to prevent and minimize damage to critical infrastructure caused by nation state cyber-attacks is imperative. The public and private sectors should continue to work together to help advance the goals of cybersecurity, and to promote safety, security, and economic prosperity around the world.

Endnotes

1. Jing de Jong-Chen is a Partner and General Manager of Global Cybersecurity Strategy and Bobby O'Brien is a Senior Cybersecurity Strategist in the Digital Trust Group of the Corporate, External and Legal Affairs Division at Microsoft Corp. Jing serves as a Board Advisor for the Woodrow Wilson Center Technology and Innovation Program. The opinions expressed in this article are those solely of the authors. The authors wish to thank Amanda Craig and Paul Nicholas for their review and contribution.
2. This definition, which was later adopted in the NIST Cybersecurity Framework, has its origin in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)).
3. For a full list of the sector specific agencies, see "Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience." White House Office of the Press Secretary. February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
4. Information related to the US National Protection and Program Directorate can be found on <https://www.dhs.gov/national-protection-and-programs-directorate> . Information of Office of Infrastructure Protection can be found on <https://www.dhs.gov/office-infrastructure-protection>
5. Federal Register – The President's "Executive Order 13636 – Improving Critical Infrastructure Cybersecurity" was released on February 19, 2013, <https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>
6. National Institute of Standards and Technology's "Cybersecurity Framework for Protecting Critical Infrastructure" can be found on <https://www.nist.gov/cyberframework>
7. It is worth noting that sector specific requirements may include national standards for security certification.
8. To learn more about Common Criteria certification, please visit <https://www.commoncriteriaportal.org/>
9. National Institute of Standards and Technology's "Cybersecurity Framework – Industry Resources" can be found here <https://www.nist.gov/cyberframework/industry-resources>
10. Digital Service Provider (DSP) requirements must be complied with by August 2017, Operator of Essential Services (OES) requirements must be complied with by May 2018 (though identification of OESs will not happen not until Nov 2018).
11. Microsoft Internal Report, 2017, "Implementing the NIS Directive."
12. "The Directive on Security of Network and Information Systems (NIS Directive)." European Commission. Accessed August 31, 2017. <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>.
13. "The Directive on Security of Network and Information Systems (NIS Directive)." European Commission. Accessed August 31, 2017. <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>.
14. "Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016, Concerning Measures for High Common Level of Security of Network and Information Systems Across the Union." Accessed August 31, 2017. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG .
15. EU released its "General Data Protection Regulation (GDPR)" policy on April 14th, 2016 <http://www.eugdpr.org/> to be enforced by May 25th, 2018.
16. Example of compliance: UK government provided guidance for the IT systems NIS Directive compliance <https://www.itgovernance.co.uk/nis>
17. Whereas the U.S. uses "critical infrastructure protection" (CIP) and the European Union uses "operators of essential services (OES), China refers to critical infrastructure protection as it relates to the ICT domain as "critical information infrastructure protection" (CIIP).
18. "2016 State Council Legislative Work Plan Notification." April 13, 2016. <http://www.gov.cn/zhengce/content/2016-04/13/content_5063670.htm>.
19. China cybersecurity policy and the draft CIIP policy required national standard-based compliance. However, in certain cases, international standards and best practices were being considered during the process of national standard development.
20. A paper on "Risk Management for Cybersecurity: Security Baselines" co-authored by Amanda Craig, Angela McKay and Kaja Ciglic, offers additional reference on policy harmonization. Forthcoming, 2017.
21. See, e.g.: <https://www.enisa.europa.eu/news/enisa-news/european-commission-opens-public-consultation-on-2018contractual-ppp2019>; https://ec.europa.eu/eusurvey/runner/NIS_Dir_IncidentReporting_DSP.

22. United Nations. Group of Governmental Experts
on Developments in the Field of Information and
Telecommunications in the Context of International Security,
July 22, 2015.
23. To learn more about Microsoft's initiatives to develop cyber
norms, please reference the blogs written by Brad Smith
"[The need for Digital Geneva Convention](#)" February 14th,
2017 and "[The Need for Urgent Collective Action to Keep
People Safe Online: Lessons from Last Week's Cyberattack](#)"
May 14, 2017.







Jing de Jong-Chen

General Manager, Global
Cybersecurity Strategy,
at Microsoft Corporation
digitalfutures@wilsoncenter.org

Jing de Jong-Chen is a Partner and General Manager of Global Cybersecurity Strategy in the Corporate, External and Legal Affairs Division at Microsoft Corp. Jing has over 20 years of experience in the high-tech sector and is responsible for Microsoft cybersecurity policy engagement and technology advancement in key strategic markets. Jing serves as Board Advisor for the Wilson Center's Science and Technology Innovation Program, Board Advisor for the Executive Women's Forum, and Vice President of the Trusted Computing Group.

The opinions expressed in this article are those solely of the author.

The Wilson Center

-  wilsoncenter.org
-  facebook.com/WoodrowWilsonCenter
-  [@TheWilsonCenter](https://twitter.com/TheWilsonCenter)
-  202.691.4000

Digital Futures Program

-  wilsoncenter.org/program/digital-futures-project
-  digitalfutures@wilsoncenter.org
-  facebook.com/WilsonCenterDFP
-  [@WilsonCenterDFP](https://twitter.com/WilsonCenterDFP)
-  202.691.4002



Bobby O'Brien

Senior Cybersecurity Strategist
at Microsoft Corporation
digitalfutures@wilsoncenter.org

Bobby O'Brien is a Senior Cybersecurity Strategist in the Corporate, External, and Legal Affairs Division at Microsoft Corp. He enjoys working on issues involving the intersection of technology, international politics, and business. He previously held roles in industry, journalism, and the think tank sector.

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027