sipri

CYBER RISK REDUCTION IN CHINA, RUSSIA, THE UNITED STATES AND THE EUROPEAN UNION

LORA SAALMAN, FEI SU AND
LARISA SAVELEVA DOVGAL

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament. Established in 1966, SIPRI provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.

The Governing Board is not responsible for the views expressed in the publications of the Institute.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

Signalistgatan 9
SE-169 70 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

CYBER RISK REDUCTION IN CHINA, RUSSIA, THE UNITED STATES AND THE EUROPEAN UNION

LORA SAALMAN, FEI SU AND
LARISA SAVELEVA DOVGAL

June 2024

sipri

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

DOI No: 10.55163/RDJQ8083

Contents

Acknowledgements

The Stockholm International Peace Research Institute (SIPRI) and the authors would like to express their sincere gratitude to the German Federal Foreign Office for supporting this project with generous funding of its cyber-related research, publications and workshops. Special thanks go to our external reviewers and our SIPRI colleagues, Dr Sibylle Bauer, Dr Wilfred Wan, Dr Vincent Boulanin and Dr Jingdong Yuan, for their constructive feedback on earlier drafts of the report. Finally, the authors also wish to express their sincere appreciation to SIPRI's Editorial Department for its significant contributions to finalizing this publication.

Summary

This report provides an overview of cyber risk reduction terminology and regulatory measures within China, Russia, the United States and the European Union (EU), based on primary source official documents. Cyber risk reduction may be defined as a combination of risk assessment, risk management and mitigation processes, through which risks in cyberspace are identified, evaluated and addressed to reduce harm and negative impacts. This paper offers a foundation to enhance engagement among the four actors on cyber risk reduction.

Chapter 2 provides an overview of official Chinese, Russian, US and EU terminology on cyber risk reduction and regulatory measures. Despite China's increasing official use of 'cybersecurity', often in connection with physical critical infrastructure, its official glossaries tend to still apply 'information security' or 'data security' when referring to risk. The use of the term 'cybersecurity risk prevention' also suggests China has an emphasis on targeting the source of the risk before the breach occurs.

Russia also has a profusion of terms related to cyber and information security risks, which include 'risk mitigation' or 'risk reduction', as well as broad terms for identifying cyber risks, such as 'negative implications' and 'intolerable events'. While limited early on to the prevention of computer attacks on information systems, recent regulations focus on continuous monitoring and security assessments, threat modelling and systematization of risk scenarios for critical information infrastructure (CII) with a particular emphasis on insulating critical assets and networks from foreign information and communication (ICT) solutions.

In the USA, cyber risk reduction has become an integral part of enterprise risk management, with official definitions of risk often omitting such qualifiers as 'cyber', 'information' or 'data'. US government reports indicate a strong emphasis on risk management for critical infrastructure. These are geared towards assuming that breaches will occur and seeking to reduce damage to physical infrastructure and increasingly to information and data integrity.

While the EU does not operate as a national actor, it has also placed an emphasis on risk management, including the identification, analysis and evaluation of risks, risk treatment and risk monitoring of network and information systems, physical critical infrastructure and ICT products and supply chains. Accordingly, it has promulgated a condensed set of measures, while seeking to promote a 'single rulebook' across all member states.

Chapter 3 compares the cyber risk reduction approaches of China, Russia, the USA and the EU. It finds that China and Russia provide clear visuals and steps, but often conflate terminology. Within China, cyberspace organizations use clear bullet points, charts and even formulas to map the factors involved in risk assessment. While these tools facilitate both implementation and training, the terms 'cybersecurity', 'information security' and 'data security' are often used interchangeably, suggesting a lack of conceptual clarity. In Russia, despite its advances in interagency cooperation and streamlined communication in information security threat assessments, terms can be vague with 'negative implications' and 'intolerable events' used interchangeably or even combined, potentially leading to confusion and reduced interoperability.

China, the USA and the EU have made strides in interagency and public–private sector coordination, but there remain jurisdictional tensions. China has established an umbrella cyberspace organization and joint official documents, which suggest domestic cooperation and interoperability, yet these tend not to specify departments or roles, making it potentially difficult for operators to decipher their responsibilities. When combined with the stringent penalties contained in its laws and orders, these

pose challenges for industry compliance and international cooperation. In the USA, government collaboration with industry is fostered by requests for comments or discussion of guidelines, yet there remains the potential for contradictory or incompatible processes among the various agencies, frameworks and recommendations. In the EU, public consultations with relevant stakeholders include policymakers and industry representatives, enhancing transparency and allowing for policy adjustments. While their compliance sequencing is clear, upcoming EU regulations suggest the potential for challenges from new risk management frameworks, contributing to duplication, redundancy and tensions related to oversight.

China, Russia, the USA and the EU have also increasingly imposed restrictions on foreign supply chains, with impacts on data and trade flows. In China, these measures are intended to address the risk of CII, core data, important data or large amounts of personal information being manipulated by foreign governments, contributing to a strong emphasis on indigenization. In Russia, concerns about the impact of foreign technologies and supply chains have led to bans on the use of foreign software and cybersecurity solutions 'developed by geopolitical rivals'. In the USA, executive orders, guides and strategies also emphasize securing supply chains to restrict the access of 'countries of concern' to bulk sensitive personal data and US government data. In the EU, supply chains and supplier relationships are targeted by risk assessments to limit 'undue influence by a third country on suppliers and service providers'. These four actors have also placed a growing emphasis on articulating liability and penalties, while eliciting potential challenges to implementation. In China, there are expansive fines and threats of the suspension of operations and the revocation of business licences for those who violate its provisions, placing a burden on public and private sector agencies. In Russia, fines, and even criminal indictments for violating requirements on CII security and personal data leaks, also set a high bar for information security management. In the USA, recent official strategies stress a liability-based model, shifting responsibility from end-users to the owners and operators of systems, the technology providers that build and service these systems and the government. And in the EU, fines and penalties for non-compliance are increasingly prominent. While serving as a potential catalyst for adoption, this approach could also create challenges for national and industry-specific implementation.

Chapter 4 provides a brief conclusion on the key points of Chinese, Russian, US and EU terminological and regulatory similarities and differences that merit greater exploration for their impact on cyber risk reduction. While China and Russia excel at clear visuals and steps for compliance, they also lack linguistic clarity, which poses challenges for implementation. China, the USA and the EU demonstrate interagency and public–private sector coordination in their regulatory frameworks, yet each faces challenges in jurisdictional overlap and clarity of roles. All four actors are integrating regulatory measures to secure their supply chains by vetting, limiting or even prohibiting foreign hardware and software, while seeking to mitigate potential misuse of data. In addressing such violations, China and Russia have more comprehensive sets of penalties that could be burdensome and hinder compliance, while the USA and the EU face obstacles to enforcing liability and penalties at their respective state and member state levels. This overview of terminology and regulatory measures provides a baseline for China, Russia, the USA and the EU to engage on their approaches to cyber risk reduction.

Abbreviations

CAC	Cyberspace Administration of China
CAPEC	Common Attack Pattern Enumeration and Classification
CERT-EU	Computer emergency response team for the EU
CII	Critical information infrastructure
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act
CISA	Cybersecurity and Infrastructure Security Agency
CISAW	China Cyber Security Review Certification and Market Supervision Big Data Centre
CNCERT/CC	China's National Computer Network Emergency Response Technical Team/Coordination Centre
CSF	Cybersecurity Framework
CSIRT	Computer security incident response team
DHS	Department of Homeland Security
DORA	Digital Operational Resilience Act
EC	European Commission
EEA	European Economic Area
ENISA	European Union Agency for Cybersecurity
ERM	Enterprise Risk Management
EU	European Union
EUCC	European Cybersecurity Certification Scheme on Common Criteria
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Modernization Act
FSS	Federal Security Service
FSTEC	Federal Service for Technical and Export Control
GDPR	General Data Protection Regulation
IT	Information technology
ICT	Information and communication technology
IoT	Internet of Things
MIIT	Ministry of Industry and Information Technology
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques and Common Knowledge
NCIRCC	National Computer Incident Response and Coordination Centre
NDRC	National Development and Reform Commission
NIS Directive	Network and Information Systems Directive
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PDE	Product with digital elements
RMP	Risk Management Process
SMSG	Securities and Markets Stakeholder Group
SOC	Security Operations Centre
SOG-IS	Senior Officials Group-Information Systems Security
US-CERT	US Computer Emergency Readiness Team

1. Introduction

China, Russia, the United States and the European Union (EU) have diverse approaches to cyber risk reduction, as is evident from their official documents and regulatory measures. Cyber risk reduction can be defined as a combination of risk assessment, risk management and mitigation processes, through which risks in cyberspace are identified, evaluated and addressed to reduce harm and negative impacts. For the purposes of this paper, the terminology used by these four actors is described but no one actor's definitions are given precedence.[1] In China, official definitions concentrate on risk assessment and in a few cases risk prevention, and 'cybersecurity', 'information security' and 'data security' are often used in tandem. 'Cybersecurity' tends to cover more physical risks, while 'information security' and 'data security' aim to address exfiltration or manipulation of content. Russia's official risk-related terminology is very broad and given lengthy definitions that cover everything from 'information security risk' to the 'risk of occurrence of negative implications', which presents challenges in terms of clarity and interoperability. US and EU directives focus on 'risk assessment' and 'risk management', often omitting qualifiers such as 'cyber', 'information' or 'data', which indicates that cyber risk reduction is part of their broader risk management frameworks.

These differences inform the design and implementation of each actor's cyber risk regulatory structure.[2] China and Russia have the most expansive networks of laws, regulations, measures, guidelines, plans, notices, certifications and assessments. The USA has a more modest, but still robust, patchwork of governmental regulations and public–private sector engagement. Of the four, the EU has the most condensed set of directives, acts, working groups and toolboxes, with acts pending and integration planned among member states. While this backgrounder focuses on the official regulatory measures issued by China, Russia, the USA and the EU, cyber risk reduction is also dependent on implementation by the private sector and in the respective provinces, special administrative regions, oblasts, states and member states. However, this is beyond the scope of this paper. Instead, the authors provide an overview of current Chinese, Russian, US and EU official cyber risk reduction terminology and key regulatory measures based on publicly available official documents. The paper concludes with a section comparing and contrasting these approaches, followed by a brief conclusion summarizing these findings. This backgrounder is intended to serve as a baseline for engagement among Chinese, Russian, US and EU experts on cyber risk reduction.

[1] Chinese language official documents were translated by Lora Saalman. Russian language official documents were translated by Larisa Saveleva Dovgal.

[2] This paper provides an overview of Chinese, Russian, US and EU terminology and regulations. For more information on each of their respective cyberspace regulatory bodies as cited in the text, see Saalman, L., Su, F. and Saveleva Dovgal, L., *Cyber Posture Trends in China, Russia, the United States and the European Union* (SIPRI: Stockholm, 2022).

2. Terminology and regulatory approaches

This section provides an overview of official Chinese, Russian, US and EU terminology on cyber risk reduction and their related regulatory measures.

China

Despite the use of the term 'cybersecurity' (网络安全) in official documents, China's official glossaries frequently use 'information security' (信息安全) or 'data security' (数据安全) when referring to risk (see box 2.1).[3] That said, the term cybersecurity is increasingly integrated into risk nomenclature by such diverse bodies as the Cyberspace Administration of China (CAC), the State Internet Information Office, the National Development and Reform Commission (NDRC), the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security, the Ministry of State Security, the Ministry of Finance, the Ministry of Commerce, the State Administration for Market Regulation, the State Administration for Radio and Television, the China Securities Regulatory Commission, the State Secrecy Bureau and the State Cryptography Administration, among others. This usage indicates an increased focus on physical damage to critical infrastructure.[4] Furthermore, China's State Council has begun to highlight 'cybersecurity risk prevention' (网络安全风险防范), placing an increased emphasis on preventing risks rather than simply responding to them.[5] This suggests targeting the source of the risk and pre-empting the threat before the breach is allowed to occur. These concepts inform the extensive laws, regulations, measures, guidelines, plans, notices, certifications and assessments that underpin China's cyber risk reduction efforts. At the strategic level, these are said to form 'four beams and eight pillars' (四梁八柱) of cybersecurity policy and regulation.[6] At the operational level, China's National Computer Network Emergency Response Technical Team/Coordination Centre (CNCERT/CC) issues regular updates on cyber risks.[7] Furthermore, there are indications of efforts to reduce the cyber risks originating from foreign supply chains. A purported Chinese official directive, 'document 79', for instance, reportedly requires state-owned companies in the finance and energy sectors, among others, to replace all foreign software in their information technology (IT) systems by 2027.[8] Leaving aside

[3] Government of China, State Council, '新时代的中国国防' [China's National Defence in a New Era], 24 July 2019; and Government of China, State Council, '中国的军事战略' [China's Military Strategy], 26 May 2015.

[4] Government of China, '中华人民共和国网络安全法' [Cybersecurity Law of the People's Republic of China], Adopted at the 24th meeting of the Standing Committee of the 12th National People's Congress, 7 Nov. 2016; National Information Security Standardization Technical Committee, '网络安全标准实践指南—网络数据安全风险评估实施指引' [Cybersecurity Standard Practice Guide: Implementation Guidelines for Network Data Security Risk Assessment], TC260-PG-20231A, v1.0-202305, May 2015; State Internet Information Office et al., '网络安全审查办法' [Cybersecurity Review Measures], Reviewed and adopted at the 20th meeting of the CAC, 16 Nov. 2021; and Office of the Central Cyber Security and Information Technology Commission and CAC, '中央网信办关于印发《国家网络安全事件应急预案》的通知' [Notice of the CAC on Issuing the 'National Cyber Security Incident Emergency Plan', no. 4, 10 Jan. 2017.

[5] China's State Council, '"十三五" 国家信息化规划' ['Thirteenth Five-Year Plan': National Informatization Plan], 15 Dec. 2016.

[6] Government of China, State Council, '新时代的中国网络法治建设' [Establishing a New Era of China's Cyber Legal Governance'], 16 Mar. 2023; Government of China, Office of the Central Cyber Security and Information Technology Commission and Cyberspace Administration (CAC), '《中国网信》杂志发表《习近平总书记指引我国网络安全工作纪实》' [*China Cyberspace* Magazine Publishes 'Record of General Secretary Xi Jinping's Guide to China's Cybersecurity Work'], 28 Sep. 2022.

[7] 国家互联网应急中心 [CNCERT/CC], [n.d.].

[8] Limits to transparency mean that this is the one case in this paper where a media report on an official document has been used. It is included due to the potential importance of 'document 79' for comparing cyber risk reduction and controls on foreign technologies among the four actors. Lin, L., 'China intensifies push to "delete America" from its technology', *Wall Street Journal*, 7 Mar. 2024.

Box 2.1. Chinese terminology

Information security risk (信息安全风险)
The possibility and impact of security incidents caused by the vulnerability of a system to human induced or natural threats.

Information security risk assessment (信息安全评估)
The process of scientifically evaluating security attributes such as the confidentiality, integrity or availability of information systems, and the information processed, transmitted and stored by them based on relevant state information security standards.

Data security risk (数据安全风险)
The potential for data security incidents and their impact on state security, public interests or the legitimate rights and interests of organizations and individuals.

Network data security risk assessment (网络数据安全风险评估)
The entire process of risk identification, risk analysis and risk evaluation of the security of network data and data processing activities.

Cybersecurity risk prevention (网络安全风险防范)
The prevention of cybersecurity risks prior to the breach occurring.[a]

[a] The following Chinese keywords were used for the research: 网络风险 (cyber risk); 网络、信息、数据安全风险管理 (cyber/information/data security risk management); 网络、信息、数据安全风险评估 (cyber/information/data security risk assessment); 网络、信息、数据安全风险控制 (cyber/information/data security risk control); 降低网络、信息、数据安全风险 (reduce cyber/information/data security risk); 减轻、缓解网络、信息、数据安全风险 (mitigate cyber/information/data security risk); 网络、信息、数据安全风险防范 (cyber/information/data security risk prevention). Those selected for the China terminology box had official definitions or explanations, based on the following sources: China Cyber Security Review Certification and Market Supervision Big Data Centre, '信息安全保障人员认证（CISAW）风险管理方向考试大纲' [CISAW Risk Management Examination Syllabus], CCRC-COP-R05:2021, n.d.; China's State Administration for Market Regulation and Standardization Administration, '信息安全技术 - 数据安全风险评估方法' [Information security technology: Risk assessment method for data security], draft released 20 Aug 2023; National Information Security Standardization Technical Committee, '网络安全标准实践指南—网络数据安全风险评估实施指引' [Cybersecurity Standard Practice Guide: Implementation Guidelines for Network Data Security Risk Assessment], TC260-PG-20231A, v1.0-202305, May 2015; and Government of China, State Council, '"十三五"国家信息化规划' ['Thirteenth Five-Year Plan': National Informatization Plan], 15 Dec. 2016.

such media reports, publicly available official regulatory documentation provides insight into China's efforts to ensure comprehensive security of its critical information infrastructure (CII) and increasingly its physical critical infrastructure.

Standards and risk assessments

Since 2006, China's State Administration for Market Regulation and Standardization has been publishing periodic, in-depth reports on information systems management requirements, information security risk assessment methods, cybersecurity protection ratings and terminology, information security risk assessment implementation, personal information security regulations, data classification and grading rules, cybersecurity standard practices and cybersecurity risk assessments.[9] Reports in the past decade

[9] China's State Administration for Market Regulation and Standardization, '金融信息系统网络安全风险评估规范' [Specification of financial information system cybersecurity risk assessment], GB/T 42926-2023, issued 6 Aug. 2023, Implemented 1 Dec. 2023; China's State Administration for Market Regulation and Standardization, '信息安全技 -术关键信息基础设施安全保护要求' [Information security technology: Cybersecurity requirements for critical information infrastructure protection], GB/T 39204-2022, issued 12 Oct. 2022, implemented 1 May 2023; and China's State Administration for Market Regulation and Standardization, '信息安全技术 - 数据安全风险评估方法' [Information security technology: Risk assessment method for data security], draft, 20 Aug 2023; China's Cyber Security Review Certification and Market Supervision Big Data Centre, '信息安全保障人员认证（CISAW）风险管理方向考试大纲' [CISAW Risk Management Examination Syllabus], CCRC-COP-R05:2021 [n.d.].

have targeted cybersecurity standards and risk assessments of financial information systems, CII and information security technology. Their definitions, charts, formulas, diagrams and step-by-step recommendations detail the specific risk assessment and management roles and responsibilities of each stakeholder. In the case of financial risk assessments, these steps include a method for evaluating the potential for an incident to occur based on the type, source, capability, timing and frequency of the threat, and the potential for vulnerability exploitation. One of the recommendations in these reports is to determine the importance of each asset based on its role in business development and the potential losses that might be incurred if it were compromised. Based on the above, the risk assessment process comprises identification of the target, formation of a working group, determination of scope, information system research, plan formulation and establishing permissions criteria. Reports on risk assessment and standards follow a systematic approach. This involves first surveying the areas where data security risks might arise, such as with data processors and data assets, or in business and information systems, data processing activities and data security protection measures; then risk identification in data security management, the data processing activity, data security technology and personal information protection; and finally risk analysis and evaluation of risk type, and degree of and potential for risk hazard. In the reports, these steps are supplemented by diagrams and charts on implementation, and evaluation methods to determine the level to which risk management standards have been met.

Cybersecurity Law

The Cybersecurity Law, adopted at the National People's Congress in November 2016, mandates that state cybersecurity and information departments—a reference to the CAC and its local branches—have a comprehensive plan for cybersecurity, and coordinate related supervision and management efforts with multiple regulatory agencies.[10] This mandate covers critical network equipment standards, certification and security reviews, and risk reduction and remediation for all providers and operators. When providers discover that their products or services have security flaws, vulnerabilities or other risks, they must immediately undertake remedial measures, notify users in accordance with regulations and report to the relevant competent authorities. Operators are tasked with: (*a*) formulating contingency plans and promptly remediating security risks, such as system vulnerabilities, computer viruses, network attacks and network intrusions; (*b*) engaging in cybersecurity certification, testing and risk assessment; and (*c*) making public information on system vulnerabilities, computer viruses, network attacks and network intrusions. The goal is to coordinate these provider and operator activities to protect CII. The law stipulates that the CAC conduct random checks and testing, engage in network security emergency drills, promote information sharing, improve cybersecurity risk assessment and emergency response mechanisms, and formulate contingency plans for cybersecurity incidents. The law escalates high-risk cybersecurity incidents to federal departments at or above the provincial level and provides for fines and the possible suspension of operations or revocation of the business licences of entities that violate its legal provisions.

National Informatization Plan

The 13th Five-Year National Informatization Plan, issued by the State Council in December 2016, focuses on cyber risk assessment, management and prevention.[11] It

[10] Government of China, '中华人民共和国网络安全法' [Cybersecurity Law of the People's Republic of China], Adopted at the 24th meeting of the Standing Committee of the 12th National People's Congress, 7 Nov. 2016.

[11] Government of China, State Council, '"十三五"国家信息化规划' [Thirteenth Five-Year National Informatization Plan], 15 Dec. 2016.

cites the need to recognize and prevent risks brought about by the application of new technologies, applications and products, including the impact of industrial robots and artificial intelligence, among other advances. The plan seeks to improve cybersecurity risk prevention and control capabilities. It envisages proactive sharing of information related to risks to economic growth and social governance that may be caused by the internet to maintain social harmony and stability. It emphasizes risk assessment and the management of military-civilian integration of cybersecurity and informatization, including through regular joint training, review and verification to meet national defence requirements. The plan also seeks to strengthen China's legal and regulatory system for the promulgation of cybersecurity, password and personal information protection laws, and the CII security assurance system. It calls for a cybersecurity review system to reduce risks in IT products and services, a catalogue of national CII, as well as formulation of guiding documents on security protection requirements for CII. The plan applies continuous threat awareness and defence capabilities to finance, energy, water conservancy, electricity supply, communications, transport and geographical data, among other things, to enhance cybersecurity capabilities. It also calls for the creation of a cybersecurity information sharing and risk reporting mechanism for government, industry and enterprises, as well as an emergency command and early warning system for major national cybersecurity incidents, supported by cybersecurity big data mining and analysis to facilitate risk monitoring, early warning, emergency response and prevention.

National Cybersecurity Incident Emergency Plan

The National Cybersecurity Incident Emergency Plan, issued by the CAC in June 2017, contains provisions for responses to red, orange, yellow and blue alerts, exhorting regions and departments to carry out continuous work on preventing cybersecurity incidents in accordance with their responsibilities, formulate and improve relevant emergency plans, carry out cybersecurity inspections, investigate hidden dangers, conduct risk assessments and disaster recovery back-ups, and improve cybersecurity information reporting and response mechanisms.[12] These efforts include precautions to be taken during important national events and meetings.

Notice for Central Government Enterprises

The Notice for Central Government Enterprises was issued by the State Council's State-owned Assets Supervision and Administration Commission in June 2017 and reposted in August 2021.[13] It stipulates that central government enterprises should comprehensively investigate and strengthen protections against cyber risks, including real-time detection and early warning, and cyber risk assessments of external services and products. It also mandates clarification of job responsibilities, the carrying out of security drills and improvement of support capabilities in the lead-up to major conferences and activities, citing the National Congress of the Communist Party of China and BRICS leaders' meetings as examples.

CII Security Protection Regulations

The CII Security Protection Regulations, adopted by the State Council in April 2021, make recommendations on the planning, construction and use of security measures to

[12] Office of the Central Cyber Security and Information Technology Commission and CAC, '中央网信办关于印发《国家网络安全事件应急预案》的通知' [Notice of the CAC on issuing the 'National Cyber Security Incident Emergency Plan', No. 4, 10 Jan. 2017.

[13] Government of China, State-owned Assets Supervision and Administration Commission of the State Council, '国务院国有资产 '关于进一步加强中央企业网络安全工作的通知' [Notice on further strengthening the cybersecurity work of central enterprises], No. 33.

protect CII from attacks, intrusions, interference and destruction, and on the punishment of illegal or criminal activities.[14] They mandate the establishment and improvement of cybersecurity management, the formulation of security protection plans and the conduct of cybersecurity monitoring and risk assessment. In accordance with national and industry cybersecurity emergency response plans, the regulations further require: (*a*) formulation of an emergency response plan; (*b*) identification of key cybersecurity roles and responsibilities; (*c*) creation of cybersecurity work assessments and proposals for reward and punishment; (*d*) conduct of education and training on cybersecurity; (*e*) creation or improvement of personal information and data security protection systems; (*f*) implementation of security management of CII design, construction, operation and maintenance; and (*g*) strengthening of emergency support systems, technical support, situational awareness and emergency command, including scenario-based, thematic and joint emergency drills.

Data Security Law

The Data Security Law, passed at the National People's Congress in June 2021, mandates state support for relevant departments, industry organizations, enterprises, educational and scientific research institutions and professional institutions with cooperation on data security risk assessment and prevention.[15] It calls for the formulation of a 'centralized, unified, efficient and authoritative data security risk assessment reporting, information sharing, monitoring and early warning mechanism'. In addition to strengthening risk monitoring when carrying out data processing activities, data processors are to conduct regular risk assessments of their activities and submit reports to the relevant competent authorities on the types and quantities of data processed, the status of data processing activities, data security risks and their countermeasures. If the relevant authorities discover significant security risks linked to data processing activities, they can interview relevant organizations and individuals, and require them to undertake corrective measures to eliminate threats.

Personal Information Protection Law

The Personal Information Protection Law, adopted at the National People's Congress in August 2021, addresses information security risks by requiring: (*a*) development of internal management systems and operating procedures; (*b*) confidential management of personal information; (*c*) adoption of encryption, de-identification and other security technical measures; (*d*) determination of operating authority for personal information processing; (*e*) provision of regular safety education and training for employees; and (*f*) implementation of emergency plans for personal information security incidents.[16]

Interagency Cybersecurity Review Measures

The Interagency Cybersecurity Review Measures were issued in December 2021 by the State Internet Information Office, the NDRC, the MIIT, the Ministry of Public Security, the Ministry of State Security, the Ministry of Finance, the Ministry of Commerce, the People's Bank of China, the State Administration for Market Regulation, the State Administration of Radio and Television, the China Securities Regulatory Commission,

[14] Government of China, State Council, '关键信息基础设施安全保护条例' [Critical Information Infrastructure Security Protection Regulations], No. 745, 30 July 2021.

[15] Government of China, '中华人民共和国数据安全法' [Data Security Law of the People's Republic of China], 10 June 2021.

[16] Government of China, '中华人民共和国个人信息保护法' [Personal Information Protection Law of the People's Republic of China], 20 Aug. 2021.

the State Secrecy Bureau and the State Cryptographic Administration.[17] They seek to prevent cybersecurity risks and to promote the use or application of advanced technologies. The focus is on national security risks, such as that: (*a*) CII could be illegally controlled, interfered with or destroyed following the use of products and services; (*b*) CII business continuity could be compromised by an interruption in product or service supply; (*c*) safety, openness, transparency, diversity or reliability of supply channels could be interrupted due to political, diplomatic, trade and other factors; (*d*) product or service providers' non-compliance with Chinese laws, administrative regulations and departmental rules could result in compromise; (*e*) core data or large amounts of personal information could be stolen, leaked, damaged, illegally used or illegally exported abroad; or (*f*) CII, core data, important data or large amounts of personal information could be affected, controlled or maliciously used by foreign governments. The measures require CII operators to submit a cybersecurity review to the Cybersecurity Review Office, in the State Internet Information Office, in anticipation of any risks that affect national security.

Data Transfer Security Assessment Measures

The Data Transfer Security Assessment Measures, adopted by the CAC in May 2022, require each agency to conduct data export risk assessments of: (*a*) the legality, legitimacy and necessity of data export, and the purpose, scope and method of data processing by the overseas recipient; (*b*) the scale, type and sensitivity of the exported data, and the risks that data export might pose to national security, the public interest and the legitimate rights and interests of individuals or organizations; (*c*) the obligations of the overseas recipient, and whether management and technical measures can ensure the security of outbound data; (*d*) the risk that data might be tampered with, destroyed, leaked, lost, transferred, illegally obtained or used during and after export; (*e*) the stipulation of data security protection responsibilities and obligations in export contracts; and (*f*) any other matters that might affect the security of data exported abroad.[18] Accordingly, those engaged in data transfer must apply for a data export security assessment, which involves a declaration, a self-assessment report on data export risks, and submission of the legal documents between the data processor and the overseas recipient. The CAC assessment takes 45 working days, with the potential for longer depending on the complexity of the application or the need for further information.

Cybersecurity Standard Practice Guidelines

The Cybersecurity Standard Practice Guidelines, published by China's National Information Security Standardization Technical Committee in May 2023, provide guidance and outline best practices on cybersecurity law, regulation, policy and standards, and cybersecurity incidents, in accordance with the Cybersecurity Law, Data Security Law and Personal Information Protection Law, among others.[19] They serve as a template for data processors, third-party vendors and regulatory authorities, evaluate security risks related to data security management, data processing activities, data security technology and personal information protection, and target security risks in relation to confidentiality, integrity, availability and rationality in data processing. According

[17] Government of China, State Internet Information Office et al., '网络安全审查办法' [Cybersecurity review measures], Reviewed and adopted at the 20th meeting of the CAC, 16 Nov. 2021.

[18] Government of China, State Internet Information Office, '数据出境安全评估办法' [Data Export Security Assessment Measures], 7 July 2022.

[19] National Information Security Standardization Technical Committee, '网络安全标准实践指南—网络数据安全风险评估实施指引' [Cybersecurity Standard Practice Guide: Implementation Guidelines for Network Data Security Risk Assessment], TC260-PG-20231A, v1.0-202305, May 2015.

to the guidelines, data security risk assessment involves: (*a*) interviewing personnel to verify implementation of systems and regulations, protective measures and safety responsibilities; (*b*) inspecting the safety management system, risk assessment report, grade guarantee evaluation report and other relevant materials on system performance; (*c*) verifying security policies on and configurations and protective measures for network environments, databases, big data platforms and related systems; and (*d*) using penetration testing and other technical means to check the status of data assets and ensure the effectiveness of protective measures.

Russia

There is a profusion of terms related to cyber and information security risks in the official Russian discourse on risk management (see box 2.2). The Central Bank of Russia uses the terms 'risk mitigation' or 'risk reduction' (снижение рисков информационной безопасности) to define cyber risks as a subcategory of information risks.[20] By contrast, the Federal Service for Technical and Export Control (FSTEC) and Russia's Ministry of Digital Development, Communications and Mass Media (Digital Ministry) use broad terms when referring to information security and information and communications technology (ICT) risks, such as 'negative implications' (негативные последствия) and 'intolerable events' (недопустимые события) respectively. The Digital Ministry uses 'cyber resilience' (киберустойчивость) or 'resilience of information infrastructure' (устойчивость информационной инфраструктуры) to discuss 'critical risks and threats to information security'.[21] This expansive scope suggests the potential for a lack of clarity and interoperability in how these definitions of risk are operationalized by various agencies. Russia's cyber risk reduction structure is underpinned by a number of laws, decrees, guidelines, orders, assessments and standards that govern its approach. At the strategic level, presidential decrees and laws provide an overarching framework that regulates information security issues pertaining to the national payment system, CII and personal data protection. With regard to CII assets, Russia has prioritized limiting its dependence on foreign technologies.[22] At the operational level, Russia's cyber risk reduction approach comprises over 100 national standards and methodologies, which include several industry-specific requirements. These are supplemented by advisories and assessments from the National Computer Incident Response and Coordination Centre (NCIRCC).[23] While early documents, such as the Personal Data Law, were limited in scope to the prevention of computer attacks on information systems, more recent regulations focus on continuous monitoring and security assessments, threat modelling and systematization of typical risk scenarios to ensure the resilience of CII.

[20] National standard ГОСТ Р 57580.3-2022, 'Security of financial (banking) operations: Information threat risk management and ensuring operational resilience, General principles'.

[21] 'Методический документ "Руководство по организации процесса управления уязвимостями в органе (организации)" (утв. Федеральной службой по техническому и экспортному контролю 17 мая 2023 г.)' [Methodological document 'Guidance on the organization of a vulnerability management process in a body (organization)', approved by the Federal Service for Technical and Export Control on 17 May 2023]; Ministry of Digital Development, Communications and Mass Media of the Russian Federation, Методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием [Methodological recommendation on digital transformation of state corporations and companies with state participation], n. d.

[22] Указ Президента РФ от 30 марта 2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [Presidential Decree no. 166 'On measures to ensure technological independence and security of critical information infrastructure of the Russian Federation'], 30 Mar. 2022.

[23] Russian National Computer Incident Response and Coordination Centre (NCIRCC); Национальный координационный центр по компьютерным инцидентам, 'Рекомендации по компенсации ИТ-рисков для компаний и организаций Российской Федерации в условиях санкционных ограничений' [Recommendations on ICT risk compensation for companies and organizations of the Russian Federation in the context of sanctions], 19 Mar. 2022.

Furthermore, development of new measures, including on the cybersecurity of open software repositories, increasingly occurs through interagency consultations between the Digital Ministry, the FSTEC and the Federal Security Service (FSS), as well as in coordination with cybersecurity and ICT companies.[24]

Personal Data Law

Signed in July 2006, the Personal Data Law seeks to make the processing of personal data more secure through the: (*a*) identification of threats to the security of personal data in information systems; (*b*) application of relevant and trusted organizational and technical security measures; (*c*) detection of unauthorized access to personal data, and measures to locate, prevent and eliminate the consequences of computer attacks on personal data information systems and respond to computer incidents; (*d*) recovery of personal data modified or destroyed through unauthorized access; and (*e*) control of access to personal data.[25] A follow-on document published by the FSTEC in February 2013, the Security of Personal Data in Information Systems Specifications, contains specific measures on the security of personal data.[26] These include on the identification and authentication of who has access to personal data and through which means, managing access control, use of trusted software, security event logging, antivirus defence, incident detection and response, personal data security analysis, ensuring the integrity and availability of information systems and personal data, and protection of the virtual environment, technical means and communication and data transfer systems.

Security of CII Law

Russia adopted a law to reduce risks to CII assets in July 2017.[27] The Security of CII Law stipulates that these risk reduction responsibilities should be divided between the CII organizations that own these assets, the FSTEC and the FSS. Under this law, critical information infrastructure organizations (субъекты критической информационной инфраструктуры) are identified as state bodies and institutions or individual entrepreneurs that own information systems, ICT networks and automated control systems operating in key sectors such as healthcare, energy and banking, as well as organizations that ensure interaction of these systems or networks. These CII organizations must categorize their assets and report this to the FSTEC, which is responsible for compiling a register of CII assets, and investigating and reporting on any vulnerabilities of the software and equipment used by CII organizations. Finally, NCIRCC, which reports to the FSS, must conduct a regular security assessment of all critical information assets.

[24] Ministry of Digital Development, Communications and Mass Media of the Russian Federation, 'Методические рекомендации по обеспечению информационной безопасности при создании и эксплуатации открытых репозиториев программного обеспечения [Methodological recommendations on ensuring information security in the creation and operation of open software repositories]', 29 Mar. 2023.

[25] 'Федеральный закон от 27 июля 2006 года N 152-ФЗ «О персональных данных» (с изменениями на 6 февраля 2023 года) [Federal Law no.152 of 27 July 2006 (as amended on 6 Feb. 2023) 'On personal data'].

[26] 'Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Федеральной службой по техническому и экспортному контролю 18 февраля 2013 г.)' [Composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems, approved by the Federal Service for Technical and Export Control on 18 Feb. 2013], 18 Feb. 2013.

[27] 'Федеральный закон от 26 июля 2017 №187-ФЗ 'Обезопасности критической информационной инфраструктуры Российской Федерации' [Federal Law no.187 'On the security of critical information infrastructure of the Russian Federation'], 26 July 2017.

Box 2.2. Russian terminology

Information security risk, risk of realization of information threats (риск информационной безопасности, риск реализации информационных угроз)
The possibility of information threats, and their implications, caused by deficiencies in operational reliability and information protection, deficiencies in the software of automated systems and applications, as well as inconsistencies in these processes with the activities of an organization.

Cyber risk (киберриск)
The risk of deliberate actions by the employees of an institution and/or third parties using software and/or hardware aimed at the institution's information assets to disrupt and/or halt their functioning and/or threaten the security of information processed and stored, including for the purposes of unauthorized appropriation, theft, change or deletion of data and other information.

Information security threat (угроза безопасности информации)
A set of conditions and factors that create the potential or actual danger of an information security breach.

Information security risk management (управление рисками информационной безопасности)
Coordinated actions to direct and manage activities related to the risk of occurrence of information threats in a financial organization.

Risk of realization of negative implications (риск реализации негативных последствий)
Risks resulting in violations of citizens' rights; damage to national defence, security, law and order, as well as state-level activities in the social, economic, political and environmental spheres; and the occurrence of financial, production, reputational or other risks or types of damage to an information owner or operator.

Risk of realization of intolerable events (риск реализации недопустимых событий)
Risks resulting from actions by malicious actors that make it impossible to achieve operational and strategic objectives or result in a prolonged disruption to core business activities.[a]

[a] The following Russian keywords were used for research: Риск информационной безопасности (information security risk); Киберриск (cyber risk); Киберустойчивость (cyber resilience); Снижение рисков информационной безопасности (risk mitigation or risk reduction); Повышение киберустойчивости (enhancing cyber resilience); Риск реализации негативных последствий (risk of realization of negative implications); Риск реализации недопустимых событий (risk of realization of intolerable events); Снижение актуальности угроз информационной безопасности (reduction of the relevance of information security threats); Управление рисками информационной безопасности (information security risk management); Оценка рисков информационной безопасности (information security risk assessment); Угроза безопасности информации (Information security threat); Уязвимость (vulnerability). Those selected for the Russia terminology box had official definitions or explanations, based on the following sources: National standard ГОСТ Р 57580.3-2022, 'Security of financial (banking) operations. Information threat risk management and ensuring operational resilience, General principles', 1 Feb. 2022; 'Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)' [Methodology for assessing threats to information security, approved by the Federal Service for Technical and Export Control on 5 February 2021], 5 Feb. 2021; 'Методический документ "Руководство по организации процесса управления уязвимостями в органе (организации)" (утв. Федеральной службой по техническому и экспортному контролю 17 мая 2023 г.)' [Methodological document 'Guidance on the organization of a vulnerability management process in a body (organization)', approved by the Federal Service for Technical and Export Control on 17 May 2023]; and Ministry of Digital Development, Communications and Mass Media of the Russian Federation, Типовое техническое задание на выполнение работ по оценке уровня защищенности информационной инфраструктуры [Standard technical specification for assessing the level of protection of information infrastructure], 3 Jun. 2022.

Guidelines on Information Security Threat Assessment

The Guidelines on Information Security Threat Assessment, published by the FSTEC in February 2021, provide tools for developing threat models that can be modified to enhance industry-specific methods for information security risk assessment.[28] The document addresses information security threats such as potential violations and intrusions, but threats related to security breaches of cryptographic means of information protection are beyond its scope. The guidelines detail a systematic process that involves (*a*) identifying the negative impacts of information security risks through the creation of information security risk scenarios; (*b*) determining the relevance of these risks; (*c*) maintaining an inventory of systems and networks and identifying possible targets; (*d*) identifying the sources of threats from foreign intelligence services, terrorist groups, competitors, software developers and former employees; (*e*) assessing the capabilities of potential intruders; and (*f*) evaluating the possibility that information security risks might occur. Information security threat assessment is based on Russian legislation and regulations, FSTEC's threat database and other publicly available vulnerability lists, such as Common Attack Pattern Enumeration and Classification (CAPEC) and MITRE Adversarial Tactics, Techniques and Common Knowledge (MITRE ATT&CK). The results are collated in an information security threat model, which is a description of systems and networks, as well as actual information security risks such as personal, corporate and state level risks and their corresponding possible negative implications. The guidelines also recommend forming an expert group to assess information security threats. The group should comprise experts in information protection, digital transformation, communications exploitation and information operation, and assess the potential negative implications of information security threats as well as the goals and strategies of those seeking to exploit those threats.

Presidential Decree on Technological Independence and the Security of CII

The Presidential Decree on the Technological Independence and Security of CII of March 2022 forbids the use of foreign software in CII facilities after January 2025.[29] It builds on previous efforts to insulate Russian CII from external risks, such as a presidential decree in May 2018 and related recommendations by the Digital Ministry.[30] In May 2022, it was followed up by a presidential decree mandating all CII organizations to establish an information security department, and making the head of each organization personally responsible for ensuring the security of CII assets.[31] In March 2024, the Digital Ministry introduced a bill authorizing the categorization of CII assets by the

[28] 'Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.) [Methodology for assessing threats to information security, approved by the Federal Service for Technical and Export Control on 5 February 2021], 5 Feb. 2021.

[29] 'Указ Президента РФ от 30 марта 2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [Presidential decree no. 166 'On measures to ensure technological independence and security of critical information infrastructure of the Russian Federation'], 30 Mar. 2022

[30] 'Указ Президента Российской Федерации от 07.05.2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [Presidential Decree no. 204 of 7 May 2018, 'On the national goals and strategic objectives of the development of the Russian Federation for the period until 2024']; Ministry of Digital Development, Communications and Mass Media of the Russian Federation, 'Методические рекомендации по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения' [Methodological recommendations on transition of state-owned companies to the predominant use of domestic software, including domestic office software], 20 Sep. 2018.

[31] 'Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»' [On additional measures to ensure information security of the Russian Federation'], 1 May 2022.

ministry rather than organizations themselves, to ensure that the correct procedures are followed for transitioning to Russian software and hardware at CII facilities.[32]

Technical Specification for Infrastructure Security Assessment

The Technical Specification for Infrastructure Security Assessment, published by the Digital Ministry in June 2022, assesses the level of protection provided for an organization's information infrastructure.[33] A general security assessment is to be followed by an investigation of traces of successful compromises of the information infrastructure conducted by a cybersecurity contractor. The tasks include compiling a register of intolerable events at the organizational level; an assessment of the likelihood of the intolerable risk scenarios occurring by modelling targeted attacks on perimeter infrastructure and web applications; an assessment of countermeasures; and development of a roadmap for modernization of the information infrastructure to enhance its security. In August 2022, the Digital Ministry announced plans to create an open-access register of typical and systematized intolerable scenarios categorized by industry, based on the reporting of CII organizations.[34]

Information Security Risk Management Standard

Launched by the Central Bank in February 2023, the Information Security Risk Management Standard makes recommendations primarily to banking and other financial organizations, but also to other organizations that provide information services, on: (*a*) information risk detection and identification; (*b*) planning and implementation, and control and improvement of measures to increase the efficiency of information security risk management and reduce the negative impact of information security risk; (*c*) detection of specific incidents that indicate information security risks; (*d*) awareness-raising of information threats; and (*e*) establishment and implementation of control and audit programmes on risk scenario analysis.[35]

Guidelines on vulnerability management

In May 2023, the FSTEC published methodological guidelines on a framework for detailed regulations and standards on vulnerability management targeted at vulnerabilities identified in information systems software and hardware, automated control systems, ICT networks and the infrastructure of data processing centres, in line with each organization's specific operational requirements.[36] They prescribe: (*a*) monitoring of vulnerabilities and an assessment of their importance; (*b*) assessment of threat criticality; (*c*) determination of methods and priorities for vulnerability remediation, such as software updates and the application of other information protection measures; and (*d*) mitigation of vulnerabilities and assessment of mitigation processes. The guidelines also specify which members of an organization should be involved at each stage of the process and provide concrete examples of actions to be carried out. They set out a mitigation timeline of 24 hours for critical risk scenarios, seven days for high-risk scenarios, four weeks for medium-risk scenarios and four months for low-risk scenarios.

[32] 'КИИ на стол' [CII is put on the table], Kommersant, 21 Mar. 2024.

[33] Ministry of Digital Development, Communications and Mass Media of the Russian Federation, 'Типовое техническое задание на выполнение работ по оценке уровня защищенности информационной инфраструктуры' [Standard technical specification for assessing the level of protection of information infrastructure], 3 June 2022.

[34] 'Для госсектора открывается невозможное' [The public sector discovers the impossible], *Kommersant*, 23 Aug. 2022.

[35] National standard ГОСТ Р 57580.3-2022 (note 20).

[36] 'Методический документ "Руководство по организации процесса управления уязвимостями в органе (организации)" (утв. Федеральной службой по техническому и экспортному контролю 17 мая 2023 г.)' [Guidelines for organization of the vulnerability management process in a body (organization), (approved by the Federal Service for Technical and Export Control on 17 May 2023)], 17 May 2023.

Information Security Monitoring Order

In May 2023, the FSS signed an order mandating that security monitoring is to be carried out by its Information Protection and Special Communication Centre, rather than the NCIRCC, to 'assess the ability of information resources of bodies (organizations) to withstand information security threats'.[37] It tasks CII bodies with reporting to the FSS the domain names and external network addresses of all the information resources they own or use. FSS continuous monitoring is to involve the collation and analysis of information and information resources owned or used by CII organizations, the identification of operational services and the detection of vulnerabilities, as well as security assessments of information resources. Under the order, the FSS reserves the right to carry out its investigations and monitoring remotely without prior notification.

Assessment of Technical Information Protection and CII Security Methodology

The Assessment of Technical Information Protection and CII Security Methodology, published by the FSTEC in May 2024, suggests a framework for assessing the level of protection of critical information assets in state organizations and CII bodies, and of compliance with minimum requirements for protection against typical information security threats.[38] To determine the level of protection of information assets, the methodology suggests using indicators on organizational structure and management, user protection, information systems protection, and information security monitoring and response. The assessment must be based on an organization's internal documentation and policies regulating the security of its information assets, internal and external assessments of information security protection levels, an inventory of information systems, analysis of the performance of deployed software and hardware, and employee interviews. The results of such an assessment can be provided to the FSTEC voluntarily. If requested by the FSTEC, however, an assessment must be reported within 30 days.

The United States

In the USA, cyber risk reduction has become an integral part of enterprise risk management.[39] Glossaries from the National Institute of Standards and Technology (NIST) place risk assessment, risk mitigation and risk evaluation under this broader heading

[37] 'Приказ ФСБ России от 11 мая 2023 г. № 213 «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими»' [Order of the Federal Security Service of Russia no. 213 'On approval of the procedure for monitoring the security of information resources belonging to federal executive authorities, supreme executive bodies of state power of constituent entities of the Russian Federation, state funds, state corporations (companies), other organizations established on the basis of federal laws, strategic enterprises, strategic joint-stock companies and backbone organizations of the Russian economy, legal entities that are subjects of critical information resources, and other organizations established on the basis of federal laws'], 11 May 2023.

[38] 'Методический документ "Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" (утв. Федеральной службой по техническому и экспортному контролю 2 мая 2024 г.) [Methodology for assessing technical information protection and the security of significant objects of critical information infrastructure of the Russian Federation (approved by the Federal Service for Technical and Export Control on 2 May 2024]', 2 May 2024.

[39] NIST, 'Integrating Cybersecurity and Enterprise Risk Management (ERM)', NIST IR 8286, Oct. 2020.

of 'risk management' (see box 2.3).[40] In fact, US official definitions of risk tend to omit the qualifiers 'cyber', 'information' or 'data' altogether. Over the past decade, US government reports have indicated a growing emphasis on risk management for critical infrastructure, such as supply chains in manufacturing, energy supply, communications, pipelines and other industries.[41] Thus, while terms such as 'resilience management' appear periodically, risk management is most commonly used with resilience as a subcategory.[42] This priority has extended across presidential administrations and generated a network of executive orders, strategies, acts, frameworks, guides and ventures.[43] At the strategic level, this ever-evolving network of regulations prioritizes public and private sector coordination to mitigate risk, with a recent emphasis on the role and liabilities of the private sector.[44] At the operational level, the US Computer Emergency Readiness Team (US-CERT) provides frequent alerts and guidance on anticipating and mitigating emerging risks, while there have also been periodic targeted bans that address supply chain risks.[45] Under the US risk-based approach to cybersecurity, there is an emphasis on zero trust architecture and supply chain security, in the assumption that breaches will occur. This approach requires government and industry to reduce the harmful impact of such cyber incidents on critical infrastructure, and increasingly on information and data integrity.

SAFECOM Guide

Formed following the events of 11 September 2001 and managed by the Cybersecurity and Infrastructure Security Agency (CISA), SAFECOM provides a guide to cybersecurity risk assessment to help public safety organizations understand the cyber-related risks to their operations, which covers mission, functions, critical service, image and reputational damage, and risks to organizational assets and individuals.[46] The SAFECOM guide has customizable reference tables to help organizations identify and document personnel and resources at each step of cyber risk assessment to meet operational and mission needs, improve overall resilience and 'cyber posture', and qualify for cyber insurance coverage. It contains guidelines on identification and documentation of: (*a*) network asset vulnerabilities through characterization or inventory of network components and infrastructure; (*b*) sources of cyber threat intelligence, such as the US-CERT alerts, CISA's Known Exploitable Vulnerabilities

[40] NIST, 'Risk management framework (RMF)', [n.d.]; NIST 'Risk Management Framework for Information Systems and Organizations', Revision 2, NIST Special Publication 800-37, Dec. 2018; NIST, 'risk mitigation', [n.d.]; NIST, 'risk assessment', [n.d.]; and Stoneburner, G., Goguen, A. and Feringa, A., *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*, NIST, Special Publication 800-30, July 2002.

[41] NIST, 'Framework for Improving Critical Infrastructure Cybersecurity', Version 1.1., 16 Apr. 2018; Boyens, J. et al., *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, NIST Special Publication, NIST SP 800-161r1, May 2022; NIST, 'Information Security', *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, Mar. 2011; Dempsey, K. et al., *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*, NIST Special Publication 800-137A, May 2020; Executive Office of the President, 'Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure', Executive Order 13800, 11 May 2017; Powell, M. et al., *Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector*, NIST Special Publication 1800-10, Mar. 2022; Office of Cybersecurity, Energy Security and Emergency Response, 'Cybersecurity Risk Management Process (RMP)', US Department of Energy, [n. d.]; and Federal Communications Commission, 'Cybersecurity Risk Reduction', 18 Jan. 2017.

[42] US Government Accountability Office, *'Enterprise Risk Management': Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, GAO-17-63, Dec. 2016.

[43] NIST, 'Integrating cybersecurity and Enterprise Risk Management (ERM)', NIST IR 8286, Oct. 2020.

[44] The White House, *National Cybersecurity Strategy*, Washington, DC, 1 Mar. 2023.

[45] US Department of Homeland Security, 'US-CERT: United States Computer Readiness Team', [n.d.]; Federal Register, 'Federal Acquisition Regulation: Use of Products and Services of Kaspersky Lab', 10 Sep. 2019.

[46] SAFECOM, 'SAFECOM Guidance on Emergency Communications Grants', [n. d.].

Catalogue, InfraGard, the National Capital Region Threat Intelligence Consortium and the Multi-State Information Sharing and Analysis Center, among others; (*c*) internal and external threats within internal processes, and records related to administrative privileges, activity logs and supply chains; (*d*) potential mission impacts on all system dependencies and shared resources should a cyber incident occur; (*e*) threats, vulnerabilities, likelihoods and impacts for evaluating and updating cyber measures in response to new technologies and methods; and (*f*) risk responses, such as maintaining and updating contact information to expedite cyber incident response times to CISA Cybersecurity Advisors, US-CERT, the FBI and the Statewide Interoperability Coordinator, among others.[47]

Executive Order on Improving Critical Infrastructure Cybersecurity

The Executive Order on Improving Critical Infrastructure Cybersecurity, issued by the Obama Administration in February 2013, advocates government partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and to collaboratively develop and implement risk-based standards.[48] Its measures include expansion of the programmes that bring private sector subject-matter experts into government on a temporary basis to provide advice on the content, structure and types of information useful to critical infrastructure in reducing and mitigating cyber risks. It tasks the Secretary of Commerce to direct the NIST Director to lead development of a framework to reduce cyber risks to critical infrastructure. This framework comprises sets of standards, methodologies, procedures and processes that align policy, business and technology to address cyber risks through voluntary consensus and industry best practices under the NIST Act and the National Technology Transfer and Advancement Act. The framework identifies: (*a*) cross-sector security standards and guidelines for critical infrastructure; (*b*) areas for improvement in collaboration with relevant sectors and standards-developing organizations; and (*c*) technology neutral guidance to enable critical infrastructure sectors to benefit from a competitive market for products and services that meet cyber risk standards. It also tasks the Secretary of Homeland Security, within 150 days, to use a risk-based approach to identify critical infrastructure in which a cybersecurity incident could pose catastrophic effects to public health, safety, economic security or national security.

Federal Information Security Modernization Act

The Federal Information Security Modernization Act was passed in 2014, amending the 2002 version.[49] It (*a*) authorizes the Department of Homeland Security (DHS) to provide operational and technical assistance to other executive branch civilian agencies on request; (*b*) places the federal information security incident centre, a function fulfilled by US-CERT, within the DHS by law; (*c*) provides for DHS technology deployments to other agencies' networks on request; (*d*) directs the Office of Management and Budget (OMB) to revise its policies on notification of individuals affected by federal agency data breaches; (*e*) requires agencies to report major information security incidents and data breaches to Congress both annually and as they occur; and (*f*) simplifies existing reporting to eliminate inefficient or wasteful reporting, while adding new reporting

[47] US Cybersecurity and Infrastructure Security Agency (CISA), 'Cybersecurity Alerts & Advisories', [n. d.]; CISA, 'Known Exploited Vulnerabilities Catalog', [n.d.]; and Federal Bureau of Investigation (FBI), 'Field Offices', [n.d.].

[48] The White House, Office of the Press Secretary, Executive Order, 'Improving Critical Infrastructure Cybersecurity', 12 Feb. 2013.

[49] US Cybersecurity and Infrastructure Security Agency (CISA), 'Federal Information Security Modernization Act', [n. d.].

Box 2.3. United States terminology

Cyber risk
Risk of financial loss, operational disruption or damage from the failure of digital technologies employed for informational and/or operational functions introduced to a manufacturing system by electronic means from the unauthorized access, use, disclosure, disruption, modification or destruction of the manufacturing system.

Cyber threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, or individuals by an information system through unauthorized access, destruction, disclosure or modification of information, and/or denial of service; also the potential for a threat source to successfully exploit a particular information system vulnerability.

Risk management framework
A structured approach used to oversee and manage risk for an enterprise.

Risk mitigation
Prioritization, evaluation and implementation of appropriate risk-reduction controls/countermeasures from the risk management process.

Risk assessment
The process of identifying risks to organizational operations, including mission, functions, image, reputation, organizational assets, individuals, other organizations and the nation, resulting from the operation of an information system.[a]

[a] The following English keywords were used for the research: Cyber risk and cyber threat; Cyber, information, data risk reduction; Cyber, information, data risk mitigation; Cyber, information, data risk assessment; Cyber, information, data risk management. Those selected for the US terminology box had official definitions or explanations based on the following sources: NIST, 'risk management framework (RMF)'; NIST, 'Risk Management Framework for Information Systems and Organizations', Revision 2, NIST Special Publication 800-37, Dec. 2018; NIST, 'risk mitigation'; NIST, 'risk assessment'; NIST, 'Cyber risk'; NIST, 'Cyber threat'; and Stoneburner, G., Goguen, A. and Feringa, A., *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*, NIST, Special Publication 800-30, July 2002.

requirements for major information security incidents.[50] To ensure compliance, agencies are directed to create security plans, to implement security controls and to conduct regular security risk assessments. These are to be accomplished by outlining roles and responsibilities; providing training, tracking and monitoring of progress; defining steps and timelines for cyber incident response; and creating protocols for investigating and mitigating cyber risks and reporting breaches. Each agency is to maintain a comprehensive and up-to-date view of its own networks and those of its vendors. Vendors must also adhere to Federal Information Security Modernization Act (FISMA) security requirements.

NIST Risk Management Framework

The NIST Risk Management Framework, launched by NIST in November 2016, is a process for managing security and privacy risk linked to a suite of NIST standards and guidelines to support implementation of risk management programmes for meeting FISMA requirements.[51] It has seven steps: (*a*) preparation through essential activities that enable an organization to manage security and privacy risks; (*b*) categorization of

[50] US Cybersecurity and Infrastructure Security Agency (note 49).

[51] National Institute of Standards and Technology (NIST), 'NIST Risk Management Framework', [n.d.]; and NIST, 'NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations', Sep. 2020.

the system and the information processed, stored and transmitted based on an impact analysis; (*c*) selection of a set of NIST SP 800-53 controls to protect the system based on risk assessments; (*d*) implementation of these controls and documentation of how they have been deployed; (*e*) assessment of whether the controls are in place, operating as intended and producing the desired results; (*f*) authorization of system operation according to a risk-based decision made by a senior official; and (*g*) continuous monitoring to control implementation and risks to the system.

Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

The Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, issued by the Trump Administration in May 2017, holds agency heads accountable for implementing risk management measures commensurate with the risk and magnitude of harm from unauthorized access, use, disclosure, disruption, modification or destruction of IT and data; and for ensuring that cybersecurity risk management processes are aligned with strategic, operational and budgetary planning processes.[52] It mandates each agency head to use the NIST Framework for Improving Critical Infrastructure Cybersecurity to manage the agency's cybersecurity risk and to provide a risk management report to the Secretary of Homeland Security and the Director of the OMB within 90 days. Reporting includes on the risk mitigation decisions made by each agency head, such as strategic, operational and budgetary considerations; any accepted risk from unmitigated vulnerabilities; and action plans to implement the NIST framework. Furthermore, the Secretary of Homeland Security and the Director of the OMB are to jointly assess each agency's risk management report and align their policies, standards and guidelines with the NIST. It also stipulates that the executive branch provide support to owners and operators of national critical infrastructure, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the FBI, the heads of sector-specific agencies and agency heads. The executive order further tasks the Secretary of Defense, the Secretary of Homeland Security and the Director of the FBI, in coordination with the Director of National Intelligence, to recommend mitigation measures for the cyber risks facing the national defence industrial base, including its supply chain, and US military platforms, systems, networks and capabilities.

NIST Cybersecurity Framework

The NIST Cybersecurity Framework, published by NIST in April 2018, assists organizations to identify security gaps and meet cybersecurity regulations through voluntary compliance.[53] Its Quick Start Guide itemizes core functions, such as identification of critical enterprise processes and assets; documentation of information flows; maintenance of a hardware and software inventory; establishment of cybersecurity policies, including roles and responsibilities; and identification of threats, vulnerabilities and risks to assets. In February 2022, NIST issued a public request for information seeking feedback and suggestions on how to improve the existing framework to yield a 2.0 version in 2024.

[52] Federal Register, Executive Office of the President, 'Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure', Executive Order 13800, 11 May 2017.

[53] National Institute of Standards and Technology (NIST), 'Framework for Improving Critical Infrastructure Cybersecurity' (note 41); NIST, 'CSF 1.1 Quick Start Guide', [n. d.]; and NIST, 'NIST's Journey to CSF 2.0', [n.d.].

Systemic Cyber Risk Reduction Venture

The Systemic Cyber Risk Reduction Venture, initiated in January 2021, seeks to drive innovation around the development of models to assess how cyber risks or incidents could affect national security.[54] It operates under the CISA's National Risk Management Center, which identifies and supports risk reduction activities through critical infrastructure risk analysis, engagement of industry and government agencies, and the provision of risk services that leverage tools, methods and partnerships to undertake strategic foresight-based operational planning. Within its mandate, systemic risk occurs when risk is spread across interdependent systems, so that the failure of one component has systemwide consequences, amplifying the impact of the cyber incident. To address this cascade effect, the venture engages cyber risk innovators, critical infrastructure owners and operators, risk managers, state and local cybersecurity professionals and 'cyber thought leaders' to undertake risk architecture development, cyber risk metric identification and risk mitigation.

Department of Homeland Security Cybersecurity Strategy

The DHS issued its Cybersecurity Strategy in May 2018.[55] Its stated aim is by 2023 to have: 'improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities'. With a strong emphasis on risk management, the primary goals are to assess evolving cybersecurity risks, protect federal information systems, protect critical infrastructure, prevent and disrupt criminal use of cyberspace, ensure effective response to cyber incidents, strengthen the security and reliability of the cyber ecosystem and improve management of DHS cybersecurity activities.

Executive Order on improving the Nation's Cybersecurity

The Executive Order on Improving the Nation's Cybersecurity, issued by the Biden Administration in May 2021, emphasizes removal of contractual barriers and increasing information sharing on threats, incidents and risks to accelerate 'incident deterrence, prevention, and response efforts' and to enable more effective defence of agencies' systems and information.[56] It advocates adoption of security best practices, advancement towards a zero trust architecture, accelerated moves to secure cloud services, centralized and streamlined access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks, and investment in both technology and personnel to match these modernization goals. It provides for standards, procedures and criteria on: (*a*) securing software development; (*b*) documenting and minimizing dependencies on products used to develop, build and edit software; (*c*) using data encryption; (*d*) monitoring of operations and alerts; (*e*) generating and providing artefacts, or work products that are produced and used during a project to capture and convey information; (*f*) maintaining accurate and current data; (*g*) determining the provenance of software code or components and controls on internal and third-party software components, tools and services; (*h*) performing regular audits and enforcement; (*i*) providing a Software Bill of Materials, 'a formal record of supply chain

[54] US Cybersecurity and Infrastructure Security Agency (CISA), 'National Risk Management Center', [n. d.]; and CISA, 'Systemic Cyber Risk Reduction Venture'.

[55] US Department of Homeland Security, 'US Department of Homeland Security Cybersecurity Strategy', 15 May 2018.

[56] The White House, Briefing room, 'Executive Order on Improving the Nation's Cybersecurity', 12 May 2021.

relationships of various components used in building software'; and (*j*) participating in a vulnerability disclosure programme.

Cyber Incident Reporting for Critical Infrastructure Act

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), issued by the Biden Administration in March 2022, requires the CISA to develop and implement regulations that require reporting on cyber incidents and ransom payments.[57] It enables CISA—which coordinates with Sector Risk Management Agencies that support individual owners and operators, information sharing and analysis organizations and sector-focused information sharing and analysis centres—to rapidly deploy resources and provide assistance to victims of attacks, analyse incoming reporting across sectors to spot trends and quickly share that information with network defenders to warn other potential victims. CIRCIA measures include a cyber incident reporting requirement, which obliges relevant entities to report cyber incidents to CISA no later than 72 hours from the time of the incident. It also mandates that any federal agency share cyber incident reports with CISA within 24 hours. The act stipulates that CISA make information, including reports received from other federal agencies, available to federal agencies within 24 hours. Finally, the CIRCIA tasks the DHS with establishing and chairing an intergovernmental Cyber Incident Reporting Council to coordinate, deconflict and harmonize federal incident reporting requirements. It authorizes initiatives related to defending against ransomware, including reporting requirements within 24 hours of any ransom payments. The act also has a Ransomware Vulnerability Warning Pilot Program through which CISA leverages existing authorities and technologies to identify systems with vulnerabilities associated with ransomware exploitation and warns entities of those vulnerabilities, enabling timely mitigation.

National Cybersecurity Strategy

The National Cybersecurity Strategy, launched by the Biden Administration in March 2023, emphasizes 'mitigating risk' by shifting responsibility from end-users to the owners and operators of systems, the technology providers that build and service these systems and the government.[58] The aim is for owners, operators and technology providers to: (*a*) protect their own systems; (*b*) ensure that private sector entities, particularly critical infrastructure, are protecting their systems; and (*c*) collect intelligence, impose economic costs, enforce the law and conduct disruptive actions to counter cyber threats. The strategy highlights the role of CISA as the national coordinator on critical infrastructure security and resilience, and the role of the OMB in developing a plan of action to secure federal systems through collective operational defence, expanded availability of centralized shared services and software supply chain risk mitigation. The software supply chain risk mitigation objective, developed in coordination with NIST, builds on the Executive Order on Improving the Nation's Cybersecurity. In addition to incorporating a zero-trust strategy, which directs federal agencies to implement multi-factor authentication, encrypt their data, gain visibility of their entire 'attack surface', manage authorization and access, and adopt cloud security tools, the strategy tasks the OMB with development of a multi-year lifecycle

[57] US Cybersecurity and Infrastructure Security Agency (CISA), 'Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)', Mar. 2022; CISA, 'Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet'; and The White House (note 44).

[58] The White House (note 44); US Department of Commerce, 'Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities', 19 Jan. 2021; US Congress, HR 1668, 'IoT Cybersecurity Improvement Act of 2020', 4 Dec. 2020; The White House (note 56); and The White House, 'National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems', 4 May 2022.

plan to accelerate federal technology modernization to eliminate legacy systems that are costly to maintain and difficult to defend. The strategy also prioritizes a 'risk-based approach to cybersecurity' across cloud service providers through implementation of the Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities. It prioritizes Internet of Things (IoT) cybersecurity through federal risk management efforts under the IoT Cybersecurity Improvement Act, maintains IoT security labelling programmes under the Executive Order on Improving the Nation's Cybersecurity and seeks to transition to interoperable quantum-resistant cryptography under the National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.

Executive Order on Preventing Access to Personal Data and US Government Data by Countries of Concern

The Biden Administration issued an Executive Order on Preventing Access to Personal Data and US Government Data by Countries of Concern in February 2024.[59] This restricts access by countries of concern to bulk sensitive personal data and US government-related data when such 'access would pose an unacceptable risk to the national security of the United States', while advocating 'open, global, interoperable, reliable, and secure flows of data across borders, as well as maintaining vital consumer, economic, scientific, and trade relationships'. In determining which types of data would constitute such a risk, the class of transactions is to be determined by the US Attorney General. Countries of concern include 'any foreign government that . . . has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of United States persons'. Among the highlighted risks, the executive order cites transmission of data via network infrastructure that is subject to the jurisdiction or control of countries of concern, including cases in which data transits a submarine cable that is owned or operated by persons owned by, controlled by or subject to the jurisdiction or direction of a country of concern, or a submarine cable is 'designed, built, and operated for the express purpose of transferring data . . . to a specific data center located in a foreign jurisdiction'. Within 120 days of the executive order, the Assistant to the President for National Security Affairs, the Assistant to the President and Director of the Domestic Policy Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Pandemic Preparedness and Response Policy, in consultation with the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, the Director of the National Science Foundation, the Director of National Intelligence, and the Director of the FBI, are to submit a report to the US president.

CISA Cybersecurity Strategic Plan 2024–2026

The CISA Cybersecurity Strategic Plan 2024–2026 outlines a vision for 'secure and resilient infrastructure' by 'leading the national effort to understand, manage and reduce risk to . . . cyber and physical infrastructure'.[60] To this end, the plan seeks to address immediate threats by increasing visibility of and the ability to mitigate cyber-security threats, 'coordinate disclosure of, hunt for and drive mitigation of critical and exploitable vulnerabilities', and 'plan for, exercise and execute joint cyber defense

[59] The White House, Briefing Room, 'Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern', 28 Feb. 2024.

[60] US Cybersecurity and Infrastructure Security Agency (CISA), 'CISA Cybersecurity Strategic Plan 2024–2026', Aug. 2023.

operations', while also coordinating 'response to significant cybersecurity incidents'. To 'harden the terrain', it seeks to 'understand how attacks really occur and how to stop them', implement measurably effective cybersecurity investments and 'provide cybersecurity capabilities and services that fill gaps and help to measure progress'. To drive security at scale, it aims to develop trustworthy technology products, 'understand and reduce the cybersecurity risks posed by emergent technologies' and 'contribute to efforts to build a national cyber workforce'.

The European Union

Unlike China, Russia and the USA, the EU does not operate as a national actor. However, it has developed a number of official documents pertaining to cyber risk (see box 2.4). Among these, the European Union Agency for Cybersecurity (ENISA) has established an inventory of risk management frameworks through its examination of models within the EU and globally.[61] From its review, ENISA determined that risk management constitutes risk assessment, which comprises the identification, analysis and evaluation of risks, risk treatment and risk monitoring.[62] Notably, instead of referring to 'risk mitigation' or 'risk reduction', as in other EU doctrines, ENISA's reports on risk management discuss 'risk treatment', which involves measures to modify risk.[63] Furthermore, while various EU regulations use the terms 'risk management' and 'risk assessment', the focus and prioritization differs. Some refer more broadly to 'cybersecurity risk management' of network and information systems, physical critical infrastructure and ICT products and supply chains, while others are more tailored to 'ICT risk management' through targeting specific sectors, such as the financial sector.[64] With this foundation, the EU has promulgated regulations, acts, directives, frameworks and toolboxes to provide direction and guidance for member states. At the strategic level, the EU has made efforts to take a more harmonized approach through a 'single rulebook' that applies acts, regulations and measures across all member states.[65] Moreover, sector-specific supervisory authorities play a central role in introducing guidelines on risk management for relevant entities within their respective domains.[66] While not legally binding, these guidelines are often regarded as of great importance by sector entities in the EU, which treat them as binding rules or as legally relevant.[67] At the operational level, among other bodies, the computer emergency response team

[61] European Commission, 'Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency'.

[62] ENISA publications related to risk management can be accessed at ENISA, 'ENISA RM/RA Framework'; and European Commission, 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union', 19 July 2016.

[63] ENISA, 'ENISA RM/RA Framework' (note 62); European Commission, 'Description of the methodology IT Security Risk Management Methodology v1.2', Directorate-General for Digital Services, 11 Aug. 2020; ENISA, 'Interoperable EU Risk Management Framework', Dec. 2022.

[64] European Commission, 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)', 27 Dec. 2022; and European Commission, 'Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011', 27 Dec. 2022.

[65] European Securities and Markets Authority, 'Final Report on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554', 17 Jan. 2024.

[66] Krüger, P. and Brauchle, J., 'The European Union, cybersecurity, and the financial sector: A primer', *Carnegie Endowment for International Peace*, 16 Mar. 2021.

[67] Securities and Markets Stakeholder Group (SMSG), 'SMSG Advice to the European Commission: Response to the Public Consultation on the Operations of the European Supervisory Authorities', 10 May 2017

Box 2.4. European Union terminology

Cyber risk
The potential for loss or disruption caused by an incident, to be expressed as a combination of the magnitude of such a loss or disruption and the likelihood of such an incident occurring.

Cyber threat
Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems or other persons.

Risk assessment
A scientific and technologically based process comprising four steps: threat identification, threat characterization, exposure assessment and risk characterization.

Risk management
A process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and, if need be, selecting appropriate prevention and control options. Measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact.

Risk treatment
Measures to modify risk appear more commonly in European Union Agency for Cybersecurity (ENISA) reports on risk management. [a]

[a] The following English keywords were used for research: Cyber risk and cyber threat; Cyber, information, data risk acceptance; Cyber, information, data, risk assessment; Cyber, information, data risk management; Cyber, information data risk treatment; Cyber, information, data risk response; Cybersecurity, information security, data security risk management; ICT risk management. Those selected for the EU terminology box had official definitions or explanations available, based on the following sources: European Parliament and Council of the European Union, 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)', EUR-Lex, 17 Apr. 2018; European Commission, 'Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)', 13 Mar. 2004; European Commission, 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union', 19 July 2016; European Commission, 'Description of the methodology IT Security Risk Management Methodology v1.2', Directorate-General for Digital Services, 11 Aug. 2020; ENISA, 'Interoperable EU Risk Management Framework', Dec. 2022; European Commission, 'Directive (EU) 2022/2555 of the European Parliament and Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)', 27 Dec. 2022; and European Securities and Markets Authority, 'Final Report on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554', 17 Jan. 2024.

for the EU (CERT-EU) collects, manages, analyses and shares information with EU institutions, bodies and agencies on threats, vulnerabilities and incidents related to ICT infrastructure.[68]

ENISA risk management framework

Working with experts from the EU member states, ENISA set up three ad hoc working groups on risk assessment and risk management and one on national risk management

[68] European Union, Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU), 'Overview', [n. d.].

preparedness between 2005 and 2010.[69] These carried out an inventory of risk management frameworks and methodologies, generating benchmarks for measuring the content of risk assessment and risk management methodologies and a framework for national risk management governance focused on CII. In the past two years, ENISA has further refined its risk management framework as: (*a*) defining the scope of risk management within an organization; (*b*) engaging in risk assessment that includes identification, analysis and evaluation of risks; (*c*) undertaking risk treatment; (*d*) employing risk acceptance; (*e*) using risk monitoring and review; and (*f*) engaging in risk communication throughout the entire process. Rather than create a new risk management framework, ENISA has sought to identify and consolidate existing frameworks based on approaches already implemented by member states and ensuring that these frameworks can be enforced effectively.

General Data Protection Regulation

Adopted in April 2016 to take effect in May 2018, the General Data Protection Regulation (GDPR) governs how personal data in the EU should be processed and transferred.[70] It is applicable to all industries. The GDPR takes a risk-based approach that encourages organizations that control the processing of personal data to conduct risk assessment and risk mitigation measures that correspond to the level of risk of their activities. It requires a data protection impact assessment to be conducted where there is a high level of risk attached to processing operations.[71] This must include an assessment of: (*a*) envisaged processing operations and the purposes of the processing; (*b*) the necessity and proportionality of the processing operations in relation to the purposes; (*c*) risk to the rights and freedoms of data subjects; and (*d*) mitigation measures such as safeguards, security measures and mechanisms to ensure the protection of personal data. The GDPR requires notification to the national supervisory authority of any personal data breach within 72 hours. This notification must include details such as the nature of the breach, a designated point of contact for further communication, the anticipated consequences, and proposed or adopted mitigation measures. This notification mechanism was first introduced by the amended ePrivacy Directive in 2009.[72]

Cybersecurity Act

The Cybersecurity Act of April 2019 sets out a voluntary EU cybersecurity certification framework for ICT products, services and processes to ensure a consistent level of security across the EU.[73] It comprises common criteria on three themes: ICT products, cloud services and 5G networks. The European Cybersecurity Certification Scheme on Common Criteria (EUCC) was launched in January 2024. While the Cybersecurity Act lays out three levels of assurance—basic, substantial and high—the EUCC only

[69] ENISA, 'Ad hoc Working Group on Risk Assessment and Risk Management'; ENISA, 'Roadmap', 30 Mar. 2006; ENISA, 'Methodology for evaluating usage and comparison of risk assessment and risk management items', 26 Apr. 2006; ENISA, 'Determining Your Organization's Information Risk Assessment and Management Requirements and Selecting Appropriate Methodologies', Sep. 2008; ENISA, 'ENISA ad hoc Working Group on National Risk Management Preparedness: consolidated report', Apr. 2011; ENISA, 'ENISA RM/RA Framework'; and ENISA, 'Risk Management Standards', 2022; and ENISA, 'Interoperable EU Risk Management Framework', Dec. 2022.

[70] European Commission, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)', 4 May 2016.

[71] European Data Protection Supervisor, 'Data Protection Impact Assessment (DPIA)', [n.d.].

[72] Crețu, C. and Dinu, L., 'Romania: Data Breach Notification Under E-Privacy Directive and General Data Protection Regulation', 21 Jan. 2021.

[73] European Commission, 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)', 7 June 2019.

has the latter two levels.[74] Implementation of the EUCC is grounded in the Senior Officials Group-Information Systems Security (SOG-IS) common criteria evaluation framework, which is used in 17 member states.[75] The maximum length of validity of the certificates is five years, during which EUCC certification bodies carry out peer assessments. A proposal has been made to amend the Cybersecurity Act by integrating managed security services—assistance for activities related to cybersecurity risk management—into the existing certification framework.[76]

NIS 2 Directive

The 2022 Network and Information Systems (NIS 2) Directive is an update of the 2016 EU Directive on Security of Network and Information Systems. It creates a baseline for mandated cybersecurity risk management measures for entities to protect their network and information systems.[77] There are ten core requirements on: (*a*) risk assessment policy; (*b*) incident handling; (*c*) business continuity and crisis management; (*d*) supply chain security; (*e*) security in network and information systems acquisition, development and maintenance; (*f*) policies and procedures for assessing the effectiveness of cybersecurity risk management measures; (*g*) basic cyber hygiene practices and cybersecurity training; (*h*) policies and procedures on the use of cryptography and encryption; (*i*) human resources security, access control policies and asset management; and (*j*) multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity. This directive applies primarily to public or private sector entities that are identified as of 'high criticality'. Exceptions apply according to the varying national specifications on how the Directive has been transposed into national legislation, and the scope of what is included as a national security priority. In the event of a significant incident, entities are required to notify their national Computer Security Information Response Team (CSIRT) or competent authority within 24 hours. Subsequently, they must provide an incident notification and initial assessment within 72 hours. Within one month of the incident notification, a comprehensive final report is required describing the incident, its impact and cause, and mitigation measures.

Digital Operational Resilience Act

Adopted in December 2022 to take effect in January 2025, the Digital Operational Resilience Act (DORA) focuses on financial information and systems security.[78] It is defined as a 'sector-specific Union legal act', which 'contains provisions requiring essential or important entities to adopt cybersecurity risk-management measures' and will take precedence over the more general NIS 2 Directive.[79] DORA will apply to 21 types of entities, such as credit, payment and electronic money institutions;

[74] European Commission, 'Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)', 7 Feb. 2024.

[75] ENISA, 'An EU Prime! EU adopts first Cybersecurity Certification Scheme', 31 Jan. 2024.

[76] European Commission, 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)', 27 Dec. 2022; and European Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services', 18 Apr. 2023.

[77] European Commission, Directive (EU) 2022/2555 (note 76).

[78] European Commission, 'Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011', 27 Dec. 2022.

[79] European Commission, Directive (EU) 2022/2555 (note 76).

account information, data reporting, crowdfunding, crypto-asset and ICT third-party service providers; investment firms; central securities depositories; trade venues and repositories; managers of alternative investment funds; management companies; insurance and reinsurance intermediaries; credit rating agencies; administrators of critical benchmarks and securitization repositories. It mandates that financial entities establish two risk management frameworks: one to address ICT risks and the other on third-party risk. The ICT risk management framework is to include strategies, policies, procedures, protocols and tools, subject to annual review, on (*a*) identification; (*b*) protection and prevention; (*c*) detection; (*d*) response and recovery; (*e*) back-up policies and procedures, restoration and recovery procedures and methods; (*f*) learning and evolving; and (*g*) communication. Financial entities are required to conduct due diligence when selecting providers and to monitor risks to ensure compliance. DORA also creates an oversight framework of ICT third party providers, which empowers the three European supervisory authorities—the European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority—to request information, conduct investigations and inspections, make recommendations and impose fines. This act requires financial entities to define, approve, oversee and take responsibility for implementation of the ICT risk management framework and to update their knowledge and skills. It also requires member states to impose administrative fines and remedial measures for non-compliance, including criminal penalties. DORA streamlines existing EU financial incident reporting obligations and establishes a unified hub for reporting major ICT-related incidents to reduce the administrative burden and duplicate reporting obligations.

ENISA interoperable risk management toolbox

The aim of the ENISA interoperable risk management toolbox, launched in 2023, is to establish an EU-wide interoperable risk management framework that allows EU member states to 'work on common threats and risk scenarios and compare their risk levels, even if they are assessed through different or proprietary tools and methods'.[80] Over 30 prominent risk management frameworks and methodologies were examined to identify best practices and the potential for interoperability. The toolbox consolidates risk management processes with international guidelines on information security risk management to support interoperability. This mapping exercise aligns the terminology, asset classifications, threat taxonomies, impacts and risk scales of various risk management methodologies to ensure standardized results.

Cyber Solidarity Act

Following a proposal by the European Parliament and the European Council in April 2023, a provisional agreement on the Cyber Solidarity Act was reached in March 2024.[81] The act addresses 'growing cybersecurity risks' and the 'overall complex threat landscape', as well as the 'clear risk of rapid spill-over of cyber incidents' by strengthening integrated EU detection, situational awareness and response capabilities, building an EU-level cybersecurity reserve with services from trusted private providers and supporting the testing of critical entities. It builds on the existing EU legislative framework, including

[80] ENISA, 'Interoperable EU Risk Management Toolbox', Feb. 2023; and ENISA, 'Compendium of Risk Management Frameworks with Potential Interoperability', Jan. 2022.

[81] European Commission, 'Commission welcomes political agreement on Cyber Solidarity Act', Press release, 6 Mar. 2024; European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents', 18 Apr. 2023; and European Commission, 'Cyber: Towards stronger EU capabilities for effective operational cooperation, solidarity and resilience', Press release, 18 Apr. 2023.

the Cybersecurity Act and its amendment, as well as the NIS 2 Directive. The act mandates deployment of a European Cyber Shield—an interconnected pan-European infrastructure of Security Operations Centres (SOCs)—to bolster the capacity for cyber threat detection and incident analysis. This body comprises the national SOCs of each member state, cross-border SOCs and a consortium of at least three member states represented by national SOCs to coordinate cyber detection and threat monitoring. The establishment of an EU Cybersecurity Reserve will create incident response services by trusted providers. Under the act, member states' cyber crisis management authorities, CSIRTs, and EU institutions, bodies and agencies will be able to request support from the EU Cybersecurity Reserve, and mission costs will be covered by the EU budget. Moreover, a Cybersecurity Incident Review Mechanism will be formed to evaluate threats, vulnerabilities and mitigation actions following significant cybersecurity incidents. Its objective is to scrutinize lessons learned and to make recommendations on improvements.

Cyber Resilience Act

Adopted by the European Parliament in March 2024, and awaiting adoption by the European Council, the Cyber Resilience Act is expected to enter into force in late 2024.[82] It establishes cybersecurity requirements for both hardware and software products with digital elements (PDEs), which are seen as presenting a 'higher cybersecurity risk by performing a function which carries a significant risk of adverse effects in terms of its intensity and ability to damage the health, security or safety of users of such products'. It mandates manufacturers to conduct cybersecurity risk assessments before introducing products to the market. These assessments must be regularly updated throughout the PDEs' support period and considered throughout the product life cycle. The act also imposes obligations on vulnerability reporting and cyber incident reporting. In the event of an actively exploited vulnerability of a PDE, manufacturers are required to notify the designated national CSIRT and ENISA within 24 hours, to be followed by another notification within 72 hours that provides detailed information about the incident and mitigation measures. A final report that provides information about the vulnerability and its impact, details of the malicious actors, and specifics on security updates and relevant measures adopted must follow in no more than 14 days. Following any severe cyber incident affecting the security of PDEs, manufacturers must promptly notify their designated national CSIRT and ENISA within 24 hours, followed by a subsequent notification within 72 hours that contains information regarding the nature of the incident, an initial assessment and mitigation measures undertaken. A final report must be filed within a month, which offers detailed insights into the incident and its impact, as well as relevant mitigation measures. Through a single reporting platform established by the act, the designated national CSIRT is tasked with disseminating notifications to all the national CSIRTs where the affected PDEs are used on their territory. Following consultations with the affected manufacturer and ENISA, the designated national CSIRT can disclose this information itself or require the manufacturer to do so to increase public awareness.

[82] European Commission, 'Position of the European Parliament adopted at first reading on 12 March 2024 with a view to the adoption of Regulation (EU) 2024/… of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)', 12 Mar. 2024.

3. Comparing and contrasting approaches

This section compares and contrasts the cyber risk reduction approaches of China, Russia, the USA and the EU based on the above-mentioned terminology and regulatory measures.

China and Russia

Clear visuals and steps but conflated terminology

In China, the CAC serves as an umbrella organization for cyberspace affairs, while related organizations publish official documents that use clear bullet points, charts and even in some cases formulas. The State Administration for Market Regulation and Standardization and the National Information Security Standardization Technical Committee use such devices in their various reports to map the interrelationships among the factors involved in risk assessment. China's Cyber Security Review Certification and Market Supervision Big Data Centre also provides a clear set of steps on certification and of requirements of information security professionals. These tools facilitate both implementation of and training on cyber risk reduction. Nevertheless, the terminology used in China can lead to confusion regarding aims. The terms 'cybersecurity', 'information security' and 'data security' are often used interchangeably in official documents, or as subsets of each another. Increasingly, cybersecurity has taken precedence as a general concept, while information security, CII and data security fall under its umbrella. Since official usage can sometimes conflate these terms, this might reflect a lack of attention to conceptual clarity.

In Russia, there is a clear division of labour among the Digital Ministry, the FSTEC and the FSS, as delineated by the Security of CII Law. The Digital Ministry is responsible for general assessments of the level of protection of information systems and security. The FSTEC oversees the information security threat database, the provision of information security recommendations and methodologies for analysing the level of information security and protection, while the FSS focuses on security monitoring. This structure facilitates interagency cooperation and streamlines communication with the CII organizations. The methodologies issued by the FSTEC contain illustrations of each step in key processes such as information security threat assessments, system- and network-level architecture and risk scenario modelling. They provide clear steps in vulnerability identification processes, list the key actors within an organization to be involved in each step and provide guidance on the qualities required of cybersecurity specialists working on information security risk assessments. The Digital Ministry's standard technical assignment contains a ranking system that awards points for reported vulnerabilities, as well as reporting templates. Despite this structural clarity, however, the language in Russian reports can be confusing or vague. For example, the terms 'negative implications' and 'intolerable events' are not just used interchangeably, but even combined, as in 'intolerable negative events'. Moreover, organizations in Russia apply a variety of terms, from the Central Bank of Russia's use of 'information security risk' to the FSTEC's 'negative implications' to the Digital Ministry's 'intolerable events'. While this might assist the heads of each CII organization when operationalizing risk reduction measures by avoiding technical jargon, the numerous terms can also lead to confusion and reduce interoperability.

China, the USA and the EU

Interagency and public–private sector coordination but jurisdictional tensions

In China, in addition to the role of the CAC in harmonizing the duties of cyberspace agencies, joint reports by the State Administration for Market Regulation and Standardization, as well as the Cybersecurity Review Measures collectively developed by 12 national organizations, are an indication of the efforts made to strengthen domestic cooperation and interoperability on cyber risk reduction. However, Chinese official documents do not tend to specify departments or roles. For example, the Cybersecurity Standard Practice Guidelines contain wording such as 'specialized security management agencies' to describe those involved in implementing risk assessments and mitigation measures. This can make it difficult for operators to decipher the risk reduction roles and responsibilities of their specific units. China's large number of laws and orders also contain penalties and can result in fines for firms or the loss of operating licences. In cases such as the Data Transfer Security Assessment Measures, lengthy timelines and stringent requirements also pose challenges for industry compliance and international cooperation. The determination of violations is complicated by the broad scope of activities and the overlapping jurisdictions of the relevant authorities, which are often not named, thereby complicating compliance.

In the USA, government collaboration with industry is typified by requests for comments or discussion of guidelines published by governmental entities, as in the case of NIST's Cybersecurity Framework and its update. Furthermore, initiatives such as the CISA National Risk Management Center's Systemic Cyber Risk Reduction Venture allow a wide range of perspectives from industry on forecasting and addressing cyber risks. SAFECOM also provides succinct and useful guides on cyber risk assessment to assist public safety organizations. The NIST Risk Management Framework and Cybersecurity Framework specify each level of responsibility and recommended outcomes, while CIRCIA's cyber incident reporting requirements are specific not only on the timelines for such activities, but also on the bodies that require notification. Nevertheless, there is still room for contradictory or incompatible processes among the various agencies, frameworks and recommendations. When conducting outreach to industry, this can lead to jurisdictional complications. For example, while NIST offers a range of useful online tools, its website contains lengthy lists of links to both current and defunct reports, which are similarly named and numbered. Industry must navigate this complexity to remain compliant.

In the EU, there have also been public consultations with relevant stakeholders, including policymakers and industry representatives. In the case of the NIS 2 Directive, over 210 feedback submissions were received during the public consultation, more than 90 from companies and approximately 60 from business associations. Another illustration is the establishment of ad hoc working groups, as with ENISA's efforts to develop two more EU Cybersecurity Certification schemes. These not only enhance transparency and allow for adjustments to policy, but also foster a sense of inclusion among stakeholders, which incentivizes compliance. Furthermore, both the NIS 2 Directive and the sector-specific DORA outline risk management measures for information and security systems. While their compliance sequencing is clear, however, the introduction of new risk management frameworks as part of upcoming EU regulations poses new challenges. Among these, the Cyber Resilience Act is anticipated to introduce cybersecurity requirements for both hardware and software PDEs, and to involve a reporting obligation and risk assessments, which are also covered by the NIS 2 Directive and DORA. This could lead to duplication and redundancy. Moreover, there are potential obstacles to harmonization among EU member states, including with

the EU's exploration of sector-specific initiatives to complement its NIS 2 Directive. While the military and defence sectors typically operate under the umbrella of national sovereignty and are usually exempt from EU regulations, the suppliers or manufacturers that serve these sectors might be subject to EU oversight, leading to potential friction.

China, Russia, the USA and the EU

Restrictions on foreign supply chains but impacts on data and trade flows

In China, Interagency Cybersecurity Review Measures are among the regulatory means intended to address the risk of CII, core data, important data or large amounts of personal information being affected, controlled or maliciously used by foreign governments. Furthermore, it is reported that a government directive known as document 79 requires the finance and energy sectors, among others, to replace all the foreign software in their IT systems by 2027, placing a strong emphasis and reliance on indigenization.

In Russia, concerns about the impact of foreign technologies and supply chains are particularly pronounced. Russia's Presidential Decree on Technological Independence and the Security of CII forbids the use of foreign software in CII facilities after January 2025, building on earlier presidential and government decrees and related recommendations by the Digital Ministry. Additional restrictive measures include a ban on the procurement of foreign software without government approval, a ban on the use of cybersecurity solutions 'developed by geopolitical rivals' and the use only of trusted software and hardware that has been certified by the FSTEC and the FSS. Russia's Guidelines on Information Security Threat Assessment aim to identify sources of threat from foreign intelligence services and terrorist groups, among others.

In the USA, executive orders from both the Trump and the Biden administrations, the SAFECOM Guide and the National Cybersecurity Strategy all emphasize securing supply chains. In particular, the Executive Order on Preventing Access to Personal Data and US Government Data by Countries of Concern restricts the access of 'countries of concern' to bulk sensitive personal data and US government-related data, while trying to balance such efforts with maintaining data flows and trade relationships.

In the EU, addressing cybersecurity risks in supply chains and supplier relationships is the focus of the NIS 2 Directive. It requires a coordinated risk assessment of critical supply chains at the EU level, both technical factors, such as critical dependencies, and non-technical factors, such as 'undue influence by a third country on suppliers and service providers' through hidden backdoors, technological lock-in or provider dependency.

Liability and penalties articulated but implementation challenges

In China, the Cybersecurity Law provides for fines and threats of the suspension of operations and the revocation of business licences for those who violate its provisions. There are 17 specific articles on legal and financial liabilities for those who write malicious programs, fail to take immediate remedial measures, neglect prompt notification of users and the authorities, cease security maintenance, end transmission or erase information, refuse or obstruct supervision and inspection or fail to provide technical support and assistance to public and national security organs. The comprehensive scope of these violations and penalties places a heavy burden on public and private sector agencies to remain compliant.

In Russia, a 2021 amendment to the Code of Administrative Offences prescribes fines for violating requirements on CII security—including the security of critical information assets, computer incident reporting and incident information exchange—and for personal data leaks. In cases of intentional damage to the security of CII assets,

including through the neutralization of existing means of protection, the provisions of the Russian Criminal Code also apply. These amendments outline penalties for CII organizations to ensure compliance, but they also set a high bar for information security management.

In the USA, the Biden Administration is working to develop a more liability-based model in its most recent National Cybersecurity Strategy. This shifts responsibility for countering cyber threats from end-users to the owners and operators of systems, the technology providers that build and service these systems and the government. While still a work in progress, this approach suggests greater alignment with other cyber actors, in particular with the EU.

In the EU, both the NIS 2 Directive and DORA incorporate fines and penalties for non-compliance. Although specific application may vary at the national level, potential financial loss could incentivize a more proactive approach to bolstering cybersecurity practices within enterprises. Moreover, the assignment of liability and accountability to the management bodies of relevant entities could serve as a catalyst for effective top-down adoption but might create challenges for national and industry-specific implementation.

4. Conclusions

China, Russia, the USA and the EU exhibit a number of terminological and regulatory similarities, but also differences that merit greater exploration for their impacts on cyber risk reduction. China and Russia excel at providing clear visuals and steps for compliance, along with penalties when these benchmarks are not met. However, China is less effective at articulating the specific departments and the roles of those that must enact cyber risk reduction. China and Russia also tend to lack linguistic clarity in official documents, which poses challenges for implementation. While their systems of governance differ, China, the USA and the EU each demonstrate cases of interagency and public–private sector coordination in establishing and implementing their regulatory frameworks in cyberspace. However, they each face challenges when it comes to jurisdictional overlap and clarity of roles, which creates tensions and a need to deconflict these cyber risk reduction initiatives. Among their similarities, China, Russia, the USA and the EU are all integrating regulatory measures to secure their supply chains by vetting, limiting or even prohibiting foreign hardware and software, while seeking to mitigate potential misuse of CII, and personal and government data. Furthermore, all four actors are at varying stages of integrating liability and penalties for non-compliance into their evolving regulations. However, China and Russia have more comprehensive sets of penalties that could become burdensome and hinder compliance, while the USA and the EU face obstacles to enforcing liability and penalties at the state and member state level respectively. This overview of terminology and regulatory measures is intended to provide a baseline for engagement among China, Russia, the USA and the EU on their respective approaches to cyber risk reduction.

About the authors

Dr Lora Saalman (United States) is a Senior Researcher within SIPRI's Armament and Disarmament, and Conflict, Peace and Security research areas.

Fei Su (China) is a Researcher in the SIPRI China and Asia Security Programme.

Larisa Saveleva Dovgal (Russia) is a Research Assistant in the SIPRI Weapons of Mass Destruction Programme.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org