sipri

SIPRI Research Policy Paper
December 2024

ENHANCING CYBER RISK REDUCTION AND THE ROLE OF THE EUROPEAN UNION

LARISA SAVELEVA DOVGAL, FEI SU AND LORA SAALMAN*

I. Introduction

As the scale, frequency and complexity of cyber incidents continue to escalate, cyber risk reduction has become not only increasingly important but also significantly more challenging.[1] Among the four major actors analysed in this paper—China, Russia, the United States and the European Union (EU)—there are shared risks despite differing threat landscapes. As identified by experts from these four actors, some common technological and targeting risks include cyberattacks on critical infrastructure, data exfiltration and privacy violations, disinformation and societal instability, ransomware attacks and supply chain exploitation.[2]

While differing in context, the similarities of cyber risks and the common obstacles in addressing them suggest an opportunity for enhancing cyber risk reduction among the four key actors. Building on a previous SIPRI report on cyber risk reduction terminology and regulatory measures, this paper first highlights common challenges to implementing cyber risk reduction among the four actors (section II). It then draws from a workshop with Chinese, Russian, US and European experts within the public sector, private sector and non-governmental organizations to explore their views on recent enhancements to cyber risk reduction regulatory measures and recommendations for the future (section III).[3] The paper concludes by suggesting approaches for the EU to enhance its role on cyber risk reduction, including among member states and through collaborative engagement with China, Russia and the USA (sections IV and V).

II. Challenges of cyber risk reduction

While there is broad recognition among China, Russia, the USA and the EU of the importance of enhancing cybersecurity, each actor's distinct economic

SUMMARY

● Cyber risk reduction within and among China, Russia, the United States and the European Union has become increasingly important, while significantly more challenging. Despite their different threat landscapes, all four cyber actors face similar cyber risks and regulatory challenges, including on terminology, data transfer and trade flows, jurisdictional tensions and penalty enforcement. Building on previous SIPRI research, including a workshop with Chinese, Russian, US and European experts, this research policy paper explores the respective views on cyber risk reduction regulatory measures and recommendations for enhancement. It concludes with approaches for the EU to enhance its role on cyber risk reduction, including among member states and through collaborative engagement with China, Russia and the USA.

[1] For more information on cyber risk reduction terminology and regulatory measures see Saalman, L., Su, F. and Saveleva Dovgal, L., *Cyber Risk Reduction in China, Russia, the United States and the European Union*, SIPRI Report (SIPRI: Stockholm, June 2024).

[2] SIPRI, 'SIPRI convenes Chinese, Russian, US and European experts for cyber risk reduction workshop', News, 26 Sep. 2024; White House, 'National Cybersecurity Strategy Implementation Plan', version 2, May 2024; Council of the European Union, 'Top cyber threats in the EU', Infographic, 27 Jan. 2024; and Chinese National Development and Reform Commission, '专家观点: 新时代网络安全的发展趋势、面临挑战与对策建议' [Expert view: Development trends, challenges and countermeasures of network security in the new era], Press release, 29 Nov. 2024.

[3] Cyber Risk Reduction Workshop, SIPRI, Stockholm, 12–13 Sep. 2024. See SIPRI (note 2).

* The authors would like to thank the German Federal Foreign Office for its support of this multi-year project.

priorities, political systems and strategic interests have contributed to their divergent approaches in addressing cyber risks. Despite these differences, these cyber actors are confronting common challenges in four primary regulatory areas: terminology, data transfer and trade flows, jurisdictional tensions and penalty enforcement.[4]

One of the core challenges arising from terminology is the inconsistency in definitions. In China, terms like 'cybersecurity', 'information security' and 'data security' are frequently used interchangeably in official documents or treated as subsets of one another, suggesting a lack of conceptual clarity that may cause confusion in international discussions or negotiations.[5] In Russia, the terminology varies across official reports and different organizations, with the Central Bank of Russia using 'information security risk', the Federal Service for Technical and Export Control (FSTEC) referring to 'negative implications', and the Ministry of Digital Development, Communications and Mass Media (Ministry of Digital Development) speaking of 'intolerable events'. While distinct terminology within each of these organizations may simplify internal communications, it also exacerbates fragmentation and hinders interoperability. Both the USA and the EU provide definitions and even online glossaries for cyber terms, but they could better harmonize the interpretation and implementation of terms such as 'cybersecurity risk management' across their various departments.

Challenges in data transfer and trade flows, particularly as they pertain to cross-border transfers and supply chain security, are priorities shared across all four actors to mitigate cyber risks. In China, there are efforts to balance cross-border data transfer risks with development, leading to restrictive regulatory tools, such as the 2022 Security Measures for Outbound Data Transfers, which evolved into the less restrictive 2024 Regulations to Promote and Standardize Cross-Border Data Flows.[6] In Russia, there are concerns over the vulnerability of critical information infrastructure (CII), with the 2022 Presidential Decree on Measures to Ensure the Technological Independence and Security of Critical Information Infrastructure in the Russian Federation forbidding the use of foreign software in CII after January 2025.[7] This presidential decree created new challenges, such as the need to acquire software and technology through illicit channels and growing digital dependency on China.[8] In the USA, the 2024 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

[4] Saalman, Su and Saveleva Dovgal (note 1).

[5] China Internet Information Centre, '《国家网络空间安全战略》全文' [Full text of the National Cyberspace Security Strategy], Xinhua, 27 Dec. 2016; and 李从玉 辛向阳 [Li Congyu Xin Xiangyang], '全媒体发展与网络意识形态安全风险防控' [Omnimedia development and internet ideological security risk prevention and control], 人民论坛网 [*People's Forum*], 3 July 2024.

[6] Chinese Government, '数据出境安全评估办法' [Security Assessment Measures for Outbound Data Transfers], 7 July 2022; and Cyberspace Administration of China, '促进和规范数据跨境流动规定' [Provisions to Promote and Regulate Cross-border Data Flows], 22 Mar. 2024.

[7] Russian Government, '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.

[8] Sherman, J., 'Russia's digital tech isolationism: Domestic innovation, digital fragmentation, and the Kremlin's push to replace Western digital technology', DFRLab, 29 July 2024.

and US government-related data.[9] This order creates pressures on data flows and trade relationships, and on small and medium-sized enterprises (SMEs) in meeting requirements. The EU focus is on supply chains and supplier relationships, with the 2022 EU Directive on Security of Network and Information Systems (NIS 2 Directive) mandating a coordinated risk assessment of critical supply chains at the EU level.[10] However, this structure has elicited capacity-building issues within member states and industry.

In terms of jurisdictional tensions, both China and the USA face the complexity of disentangling roles and responsibilities across agencies, while the EU struggles with fragmentation issues at member-state level in implementing EU legislation. In China, the management of cyber risk involves multiple departments, presenting a coordination challenge, particularly in issuing and implementing policy measures.[11] While the establishment of the Cyberspace Administration of China (CAC) and the issuance of the 2021 Interagency Cybersecurity Review Measures by 13 government agencies suggest enhanced coordination, Chinese official documents are not always clear on specific departments or roles. For example, the Cybersecurity Standard Practice Guidelines uses ambiguous terms like ‘specialized security management agencies’ to direct risk assessments and mitigation strategies.[12] The USA also faces a network of competing and cooperating agencies, yet there remain issues of conflicting or incompatible processes, frameworks and recommendations across US Cyber Command (USCYBERCOM), the National Security Agency and the Department of Homeland Security, among others. Even in cases of unified guidance such as those set out in the National Institute of Standards and Technology (NIST) standards, the NIST website provides lengthy lists of current and outdated reports, many of which have similar titles and numbering schemes. Industries must navigate this complexity to remain compliant. In the EU, despite increasing efforts to harmonize cyber risk management across member states, the introduction of new frameworks as part of forthcoming regulations may lead to overlaps and redundancies. For example, the proposed Cyber Resilience Act (CRA) is anticipated to impose cybersecurity requirements, reporting obligations and risk assessments, which are areas already addressed by the NIS 2 Directive and the Digital Operational Resilience Act (DORA). Such measures are further complicated when applied to suppliers and manufacturers for military and defence sectors and varied critical infrastructure lists across member states.[13]

Finally, enforcing penalties for non-compliance poses additional challenges. China’s Cybersecurity Law alone features 17 articles addressing legal and financial liabilities related to various cybersecurity issues that cover a

[9] White House, ‘Executive Order on Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern’, 28 Feb. 2024.

[10] Council of the EU, ‘The Council agrees to strengthen the security of ICT supply chains’, Press release, 17 Oct. 2022; Council of the EU, ‘Council conclusions on ICT supply chain security’, Outcome of proceedings, 13664/22, 17 Oct. 2022; European Commission, Directorate-General for Justice and Consumers, ‘Proposal for a Regulation laying down additional procedural rules relating to the enforcement of GDPR’, COM(2023) 348 final, 4 July 2023; and Council of the European Union, ‘Data protection: Council agrees position on GDPR enforcement rules’, Press release, 13 June 2024.

[11] 李爱君 [Li Aijun], ‘组建国家数据局释放哪些关键信号’ [What key signals does the establishment of the National Data Bureau send?], 人民论坛网 [*People’s Forum*], 15 May 2023.

[12] China Internet Information Centre et al., ‘网络安全审查办法’ [Cybersecurity review measures], Reviewed and adopted at the 20th meeting of the Cyberspace Administration of China, 16 Nov. 2021.

[13] OpenKRITIS, ‘NIS2 in EU countries’, 2024.

broad scope, including failing to implement immediate remedial measures, neglecting to promptly notify users and authorities, discontinuing security maintenance, stopping the transmission or deletion of information, obstructing supervision and inspection, and failing to provide technical support and assistance to public and national security agencies. These place a significant compliance burden on both public and private sector organizations. In Russia, the 2021 amendment to the Code of Administrative Offences and provisions of the Russian Criminal Code prescribe fines for violating requirements on CII security—including the security of critical information assets, computer incident reporting and incident information exchange—and personal data leaks, setting a high bar for information security management. The US National Cybersecurity Strategy attempts to shift the burden from end users to vendors, to reduce vulnerabilities in US digital ecosystem.[14] However, questions remain as to how vendors and the government should best cooperate when the threat actor is believed to be a nation-state, as in cases like Midnight Blizzard and Storm-0558, or when advanced persistent threats (APTs) indicate an evolution from state actors to include non-state actors.[15] In the EU, both the NIS 2 Directive and DORA incorporate fines and penalties for non-compliance, coupled with increased liability and accountability for senior management. While these measures can act as catalysts for top-down adoption, they also pose challenges for national and industry-specific implementation.[16]

III. Enhancing cyber risk reduction

Given the above regulatory challenges faced by China, Russia, the USA and the EU, this section provides an overview of some recent efforts and proposals to enhance cyber risk reduction, informed by experts hailing from each of these four cyber actors. The section addresses some of the common challenges outlined in section II, along with enhancements that target each actor's specific cyber risk reduction environment.

China

China has strived to leverage an extensive network of laws, regulations and measures to enhance its national security, improve data privacy and protection, and foster domestic innovation and development, while recognizing that the international focus on cybercrime, cyberterrorism and cyberattacks against CII are often stymied by a lack of political will among states for promoting collective efforts.[17] Despite China's comprehensive domestic framework to address cyber risk, the expansiveness, overlapping provisions and rigidities of some regulations have led to obstacles in their implementation. For example, three laws address concerns over cross-border data transfer:

[14] US Government, *National Cybersecurity Strategy* (White House: Washington, DC, 1 Mar. 2023).

[15] Jones, D., 'CISA assessing threat to federal agencies from Microsoft adversary Midnight Blizzard', Cybersecurity Dive, 5 Apr. 2024; Microsoft Security Response Center (MRSC), 'Results of major technical investigations for Storm-0558 key acquisition', MRSC Blog, 12 Mar. 2024; and Maloney, S. 'What is an Advanced Persistent Threat (APT)?', Cybereason Blog, [n.d.].

[16] Saalman, Su and Saveleva Dovgal (note 1); and Dwyer, P. C., 'Lessons from NIS2 and DORA for senior management', International Cyber Threat Task Force Blog, [n.d.].

[17] See Saalman, Su and Saveleva Dovgal (note 1).

Article 4 of the 2018 International Criminal Judicial Assistance Law, Article 36 of the 2021 Data Security Law and Article 41 of the 2021 Personal Information Protection Law.[18] These laws aim to prevent data stored within China's territory from being transferred to the justice or law enforcement institutions of foreign countries without approval from authorities within China.

Further, China's data export and management rules have proven difficult to enact, as with its Security Assessment Measures for Outbound Data Transfers, which took effect in 2022 to mitigate the risks of CII, core data, important data or large amounts of personal information being compromised, controlled or misused by foreign governments.[19] Specifically, there is a data volume threshold set by these measures that triggers compliance procedures. Companies classified as CII operators or those handling over one million individuals' personal information and exporting it overseas must undergo a security assessment by the CAC.[20] Given China's population of 1.4 billion, this threshold affects a vast number of businesses and potentially hinders development. Recognizing this, the updated 2024 Regulations to Promote and Standardize Cross-Border Data Flows raised the data volume threshold for compliance and introduced exemptions for specific cross-border data transactions.[21] To further strengthen this process, Chinese experts have suggested introducing more frequent revisions of the already enacted national regulations on cyber risk reduction to ensure their correspondence with the evolving cyber risk environment.[22]

Chinese regulations also seek to enhance coordination between the public and private sectors through recognition of commonly faced threats while emphasizing the division of labour between them. To clarify the respective roles, Chinese experts have stressed that the public sector should bear responsibility for policy formulation, supervision, CII maintenance and increasing public awareness, while private sector organizations should be responsible for maintaining the security and safety of their facilities, research and development, and training.[23] Although the sectors have distinct roles, cross-sectoral efforts to enhance information sharing also play a part. Among these, China has formulated and continues to strengthen its National Computer Virus Emergency Response Centre (CVERC) and its Computer Network Computer Emergency Response Team/Coordination Centre (CNCERT/CC), and also works regionally with the Asia-Pacific Computer Emergency Response Team (APCERT).[24] Thus, while there remains an aversion in China to public reporting of cyber incidents—thereby reducing international awareness of China's domestic threat environment—there has also been an incremental evolution of transparency through the above bodies,

[18] Chinese Government, '中华人民共和国数据安全法' [Data Security Law of the People's Republic of China], June 2021; Chinese Government, '中华人民共和国个人信息保护法' [Personal Information Protection Law], Aug. 2021; and Chinese Ministry of Justice, '中华人民共和国国际刑事司法协助法' [International Criminal Judicial Assistance Law of the People's Republic of China], 26 Oct. 2018.

[19] Chinese Government, '数据出境安全评估办法' [Security Assessment Measures for Outbound Data Transfers] (note 6).

[20] 许宁 [Xu Ning], '中国网络审查新规上路 科技企业海外上市更难了' [China's new internet censorship rules make it harder for tech companies to go public overseas], *VOA*, 16 Feb. 2022.

[21] Cyberspace Administration of China (note 6).

[22] Chinese experts, Views expressed at the SIPRI workshop (note 3).

[23] Chinese expert, View expressed at the SIPRI workshop (note 3).

[24] See CVERC, <https://www.cverc.org.cn>; CNCERT/CC, <https://www.cert.org.cn>; and APCERT <https://www.apcert.org>.

as well as in the private sector. As just one example, in 2022 the CVERC and Qihoo 360 released forensic reports and identified at least 50 APTs targeting China.[25]

To further this public and private sector collaboration, stricter vendor management is needed, according to Chinese experts who suggest making supply chain and vendor security standards mandatory.[26] In doing so, one expert even used the term 'zero trust', meaning the maintenance of strict access controls and a default position of not trusting any system.[27] This approach displays similarities to the USA's efforts to implement its own 'vendor management' and 'zero trust' approaches, particularly under the 2023 US National Cybersecurity Strategy that places more liability and responsibility onto vendors.[28] These similarities could provide a window for engagement between China and the USA. Further, they could be explored alongside such concepts raised by Chinese experts as the 'right of peaceful use', 'clean cyberspace campaign', 'cybersecurity review system' and 'holistic approach to criminal law'.[29] Greater China–USA interaction on such terminology would be useful for enhancing engagement on cyber risk reduction, particularly in light of Chinese concerns over US application of deterrence in cyberspace in operations using strategies such as 'defend/hunt forward' and 'persistent engagement' (see below in the discussion on the USA); US overreach in technology decoupling; and even the USA's sharing of lists of 'what not to attack' as 'suggesting everything else is open for the potential of a cyberattack'.[30]

Further, to address broader concerns over stability, Chinese experts note that cyber risk could be better integrated into bilateral or even multilateral strategic risk dialogues, including on CII, nuclear power plants, power grids, command and control, nuclear, space, AI and strategic stability. According to these experts, China should shift from a static or stove-piped description of risks to instead examining the interlinkage of risk and harm, and quantifying and qualifying cyber incidents and operations.[31] This would align with approaches advocated by European experts and could yield a source of collaboration between China and the EU. In this context, Chinese experts have expressed interest in learning from EU regulatory experiences,

[25] Qihoo 360, '关于西北工业大学发现美国NSA网络攻击调查报告（之一）' [Investigative report on Northwestern Polytechnical University's discovery of the US NSA's cyberattack (Part 1)], 5 Sep. 2022; Qihoo 360, '西北工业大学遭受美国NSA网络攻击调查报告（之二）' [Investigative report on Northwestern Polytechnical University's suffering from US NSA's cyberattack (Part 2)], 27 Sep. 2022; and 吕栋 [L. V. Dong], '360周鸿祎讲述：如何抓住网络攻击西工大的幕后黑手？' [Qihoo 360 Zhou Hongwei: How to catch the mastermind behind the network attack on Northwestern Polytechnical University?], *Guancha*, 15 Sep. 2022.

[26] Chinese experts, Views expressed at the SIPRI workshop (note 3).

[27] Chinese expert, View expressed at the SIPRI workshop (note 3).

[28] US Government (note 14).

[29] Chinese experts, Views expressed at the SIPRI workshop (note 3).

[30] Chinese experts, View expressed at the SIPRI workshop (note 3); 张心志 唐巧盈 [Zhang X. T. Q.], '美国进攻性网络威慑战略已严重威胁全球网络空间安全稳定' [The US offensive cyber deterrence strategy has seriously threatened the security and stability of global cyberspace], *Huanqiu*, 22 Mar. 2024; US Department of Commerce, Bureau of Industry and Security, 'Public information on export controls imposed on advanced computing and semi-conductor manufacturing items to the People's Republic of China (PRC) in 2022 and 2023', Briefing, 6 Nov. 2023; and Barkoukis, L., 'Biden actually gave Putin a list of critical infrastructure not to carry out cyberattacks on in US', *Townhall*, Tipsheet, 18 June 2021.

[31] Chinese expert and European expert, Views expressed at the SIPRI workshop (note 3); and Cyber-Peace Institute, 'Impact & harm: How do cyberattacks and operations impact civilians?', Dec. 2023.

such as the EU's General Data Protection Regulation (GDPR), creating an opportunity for knowledge sharing and capacity building.[32]

At the multilateral level, others within China have recommended greater engagement within the international community on the concepts of 'responsibility' and 'due diligence' through existing forums on norms of responsible state behaviour in cyberspace, and on application of international law in cyberspace. According to one Chinese expert, there are two legal options: (*a*) hold a state responsible under international law if cyber activity undertaken by a non-state actor can be attributed to a state (noting that such attribution is often difficult for lack of solid evidence); or (*b*) hold a state in which the cyber activity originates accountable on the basis of the due diligence principle, such that it is not necessary to prove that the state is responsible for a non-state actor's behaviour, only to prove that the state fails to carry out the process of due diligence.[33] This second option could serve as a basis for greater legal interaction on responsibility and due diligence among China, Russia, the USA and the EU.

Russia

Russia's regulatory measures have reduced some cyber risks while creating new ones. For example, measures intended to address its perceived overdependence on foreign information and communication technology (ICT) products have reduced the threat to operational resilience, posed by sanctions.[34] However, the same measures have led to a significant increase in the number of cyberattacks against domestically developed Linux-based operating systems, as well as the misuse of certified web services and their domain names once they are no longer maintained.[35] To offset these risks, Russia's Ministry of Digital Development has been developing new measures on higher standards for domestic ICT products to ensure greater alignment between domestic software and operating systems, particularly those used in CII.[36] The ministry is also discussing a bill to establish a national Telecom-CERT, a platform for cyber incident response to facilitate coordination among government cyber defence systems of the Federal Security Service (FSS), the Ministry of Digital Development and the Central Bank, and those of other banks, tech companies, marketplace providers, mobile application developers and social media platforms, among others.[37]

[32] Zhang L., '欧盟《通用数据保护条例》对我国数据安全立法的启示' [The implications of the EU General Data Protection Regulation for China's data security legislation], *Journal of Xihua University (Philosophy & Social Sciences)*, vol. 39, no. 5 (Sep. 2020); and Ran C. and Zhang M., '欧盟GDPR中数据可携权对中国的借鉴研究; Study on the data portability of EU GDPR and its reference for China', *Journal of Information Resource Management*, vol. 9, no. 2 (2019).

[33] Chinese experts, Views expressed at the SIPRI workshop (note 3).

[34] Russian expert, View expressed at the SIPRI workshop (note 3).

[35] Денисенко, А. [Denisenko, A.], 'Число атак на российские Linux выросло в 85 раз' [The number of attacks on Russian Linux has increased 85-fold], Cnews, 30 Aug. 2024; and National Computer Incident Coordination Centre (NCIRCC), 'НКЦКИ предупреждает о рисках компрометации информации при использовании браузера «Спутник»' [NCIRCC warns of risks of information compromise when using Sputnik browser], News, 2 Aug. 2924.

[36] 'Минцифры готовит новые требования к российскому ПО' [Ministry of Digital Development prepares new requirements for Russian software], Iks-media.ru, 14 Feb. 2024.

[37] 'На платформу становись: Минцифры поднимает отрасли на борьбу с киберугрозами' [Get on the platform: Ministry of Digital Development calls on industries to fight cyber threats], *Kommersant*, 21 Aug. 2024.

These regulatory steps are further enhanced by new measures on CII data protection developed by the FSTEC in August 2024. Highlighting distributed-denial-of-service (DDoS) attacks as key threats to CII security, the new regulation requires government agencies and CII organizations to store cyber incident–related data for three years, including (*a*) date and time of attack, (*b*) type of threat and its volume, (*c*) list of network addresses that may be the source of the threat, and (*d*) mitigation measures that have been implemented.[38] Moreover, with nuclear facilities as part of its core CII, Russia has developed a set of internationally accepted cybersecurity standards for nuclear power plants.[39] More broadly, in July 2024, the 'neutralization of internal threats to national security' section of the scientific committee of Russia's Security Council proposed an undisclosed range of measures to develop domestic software to counter 'destructive information, extremist and terrorist crimes', while proposing the reduction of 'the use of foreign ICTs through which AI capabilities are realized'.[40] This builds on the committee's earlier efforts to determine the conditions for establishing a specialized interdepartmental research centre on AI threats to information security and to launch AI training programs for information security specialists.[41]

To strengthen cooperation between the public sector and the private sector in reducing cyber risks, the Russian government, in cooperation with several cybersecurity companies, has increased investment in national 'bug bounty' programs targeting vulnerabilities in Russian public services.[42] The heightened threat environment since the invasion of Ukraine has prompted Russian companies to elevate the level of their cybersecurity and cyber risk reduction measures, raising awareness through employee training and surveys.[43] Following the US ban on Kaspersky's cybersecurity products, the company proposed a 'comprehensive assessment framework' for a third-party code review as a confidence-building measure to retain its position in the US market.[44] Notably, Russian companies used to conduct these code reviews with other major foreign tech companies like Microsoft, and some Russian

[38] 'Хранение данных обезопасят требованиями' [Data storage will be secured by requirements], *Kommersant*, 2 Aug. 2024.

[39] Шелофастов, Н. [Shelofastov, N.], 'Российский ГОСТ по кибербезопасности на АЭС стал международным' [Russian national standard on cybersecurity at NPPs has become an international standard], Ferra.ru, 30 July 2024.

[40] Security Council of Russia, 'Эксперты Совета Безопасности России обсудили проблемы, связанные с использованием технологий искусственного интеллекта' [Experts of the Russian Security Council discussed problems related to the use of artificial intelligence technologies], News, 3 July 2024.

[41] Security Council of Russia, 'Эксперты Совета Безопасности России обсудили вопросы использования технологий искусственного интеллекта' [Experts of the Russian Security Council discussed the use of artificial intelligence technologies], News, 11 Jan. 2024; and Security Council of Russia, 'Эксперты Совета Безопасности России рассмотрели угрозы информационной безопасности страны, связанные с применением искусственного интеллекта' [Experts of the Russian Security Council considered the threats to the country's information security posed by the use of artificial intelligence], News, 23 May 2024.

[42] 'На втором этапе «багбаунти» Минцифры специалисты нашли 100 уязвимостей в 10 госсистемах' [During the second stage of the Ministry of Digital Development's 'bugbounty', experts found 100 vulnerabilities in 10 state systems], iXBT.com, 14 June 2024.

[43] Russian experts, Views expressed at the SIPRI workshop (note 3); and Рожков, Р. [Rozhkov, R.], 'Более трети компаний пересмотрели политику в сфере кибербезопасности из-за кибератак' [More than a third of companies have revised cybersecurity policies due to cyberattacks], *Forbes* (Russia), 2 Sep. 2024.

[44] Lyons, J., 'Kaspersky says Uncle Sam snubbed proposal to open up its code for third-party review', *The Register*, 25 July 2024.

experts have suggested that these could resume in the future with Chinese companies like Huawei.[45] Furthermore, Russia has prioritized bilateral information security agreements, such as those concluded with Armenia, Azerbaijan, Belarus, China, Cuba, India, Indonesia, Kyrgyzstan, Nicaragua, Tajikistan, Turkmenistan, Vietnam and Zimbabwe, with additional ones with Ethiopia, Iran, Myanmar and Uzbekistan coming into force in 2024.[46] Agreements with other countries from Asia, Africa, the Middle East and Latin America are currently under development.[47]

While these Russian efforts are largely isolated from those of the USA and the EU, there are still some areas of potential Russian collaboration with these actors. For example, some Russian experts have argued that Russia and the USA could engage constructively on cyber risk reduction to (*a*) avoid accidents; (*b*) enhance communication, including through points of contact; and (*c*) exercise restraint.[48] Further, some Russian experts have emphasized the value in learning from the Soviet Union/Russia–USA history on nuclear arms control and creating similar epistemic communities in cyber risk reduction, while still recognizing that verification is more complicated, if at all applicable, in cyberspace. In fact, as argued by one Russian expert, cyberattacks on nuclear facilities are a common concern, particularly for Russia, China and the USA, and could serve as an area of positive engagement in the future.[49] Another Russian expert has argued that given the increased threat of cyberattacks against Russia originating in Ukraine, such engagement is critical. The expert cited official statements from the Main Intelligence Directorate of the Ministry of Defence of Ukraine that claimed to have ‘paralyzed the developer of nuclear weapons’ through alleged cyberattacks on Russian internet providers in Snezhinsk, impacting the All-Russian Scientific Research Institute of Technical Physics (VNIITF), a research institute of Rosatom State Atomic Energy Corporation.[50] Other Russian experts have stressed that rather than placing cyber issues in a silo, it would be more effective to discuss the crossover of cyber and nuclear domains, including ‘early warning’, ‘left of launch’ and ‘no go zones’ in space.[51] As with Chinese concerns over sharing lists of critical infrastructure that is ‘off limits’ to cyberattack, one Russian expert expressed concerns that such an approach may lead to a misunderstanding that ‘if you have zones where you cannot go, you are saying that other zones are where you can go’.[52]

Another Russian expert highlighted efforts by Russia to foster capacity building, giving two recent examples.[53] First, Russia held an international cybersecurity training program in August 2024, in which ‘around 70 special-

[45] Russian expert, View expressed at the SIPRI workshop (note 3).

[46] Russian expert, View expressed at the SIPRI workshop (note 3).

[47] Russian expert, SIPRI workshop (note 3); and ‘В этом году вступят в силу соглашения России по безопасности, в том числе с Ираном’ [Russia’s security agreements, including with Iran, will come into force this year], *EurAsia Daily*, 24 Apr. 2024.

[48] Russian experts, Views expressed at the SIPRI workshop (note 3).

[49] Russian expert, View expressed at the SIPRI workshop (note 3).

[50] Russian expert, View expressed at the SIPRI workshop (note 3); and ‘Хакеры ГУР парализовали работу российского разработчика ядерных боеприпасов’ [GUR hackers paralysed the work of a Russian nuclear weapons provider]’, InfoResist, 17 Aug. 2024.

[51] Russian experts, Views expressed at the SIPRI workshop (note 3).

[52] Russian expert, View expressed at the SIPRI workshop (note 3).

[53] Russian expert, View expressed at the SIPRI workshop (note 3).

ists from 20 countries' participated.[54] Second, Russia participated in the 'East Antiterror 2024' joint exercise of the Commonwealth of Independent States, held in Uzbekistan in August and September 2024, which aimed to improve actions for counteracting cyber terrorism, among other terrorist activities, through simulated attacks and responses.[55] This Russian expert also highlighted the Russian initiative, supported within the United Nations open-ended working group on international information security, to create a global intergovernmental register of contact points for the exchange of information about cyberattacks, which was launched on 9 May 2024.[56]

United States

Given US concerns over supply chain exploitation and pre-positioning of other cyber actors in its critical infrastructure systems, the USA has increasingly faced the dilemma of whether to focus on cyber incidents and operations with 'high probability with low consequence' or those with 'low probability with high consequence'.[57] The USA has worked on coordinating responsibility across its own broad and segmented cyber threat surface, with one US expert noting that if 'more than one entity owns the problem then no one owns it'.[58] Among these efforts, the 2023 US National Cybersecurity Strategy shifted responsibility for defending against cyber threats from end-users of information systems to the owners and operators—called by one US expert a shift 'from villains and victims to vendors' approach.[59] Such measures oblige the private sector to report cyber incidents with the aim of reducing risks to supply chain security, as with the Cyber Incident Reporting for Critical Infrastructure Act of 2022's timeframe of 72 hours.[60] However, some US experts have recommended further strengthening of information security requirements in government contracts, by advocating that the US Cyber Trust Mark logo should go beyond the Federal Communications Commission proposal on smart devices to apply to a broader range of ICT products.[61] A recent example is a US Department of Justice lawsuit filed against the Georgia Institute of Technology and the Georgia Tech Research Corporation alleging that they 'knowingly failed to meet cybersecurity requirements' in connection with US Department of Defense contracts.[62]

[54] The 20 countries included Bahrain, Bangladesh, Brazil, Cameroon, Indonesia, Iran, Malaysia, Oman, Pakistan, Paraguay, Saudi Arabia, Senegal, Singapore, South Africa, Syria and the United Arab Emirates. See Frank, E., 'Middle East students complete cybersecurity training', *Security Review*, 27 Aug. 2024.

[55] Commonwealth of Independent States, Anti-Terrorism Center, 'East-Antiterror—2024 joint anti-terrorism exercise of the CIS member-states', Press release, 5 Sep. 2024.

[56] Russian Embassy in Germany, 'Foreign Ministry spokeswoman Maria Zakharova on launching a global intergovernmental register to exchange data on cyber attacks/incidents', Press release, 16 May 2024.

[57] US experts, Views expressed at the SIPRI workshop (note 3).

[58] US expert, View expressed at the SIPRI workshop (note 3).

[59] US expert, View expressed at the SIPRI workshop (note 3); and US Government (note 14).

[60] CISA, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), accessed on 26 Nov. 2024.

[61] US expert, SIPRI workshop (note 3); and US Federal Communications Commission, 'Certification mark—US cybersecurity labeling program for smart devices', 8 Sep. 2023.

[62] US Department of Justice, Office of Public Affairs, 'United States files suit against the Georgia Institute of Technology and Georgia Tech Research Corporation alleging cybersecurity violations', Press release, 22 Aug. 2024.

In the context of incentivizing stakeholder compliance with national cyber risk reduction regulations, some US experts have suggested expanding tax incentives for companies to purchase equipment, enhancing cyber insurance programs, and fostering capacity-building initiatives for smaller agencies such as local offices and governments.[63] One US expert highlighted the importance of cross-jurisdictional collaboration and information sharing among US institutions responsible for cybersecurity and cyber risk reduction, citing as an example the cooperation between the Federal Bureau of Investigation, USCYBERCOM and partner agencies on such issues as foreign influence operations.[64] These exchanges would contribute to building trust and expertise, and to developing capacities for public attribution of cyber incidents, which could contribute to a more substantive discussion on cyber norms.[65]

Reflecting the evolving nature of the cyber threat environment, the USA has adapted its cybersecurity approach to move away from a ‘compliance model’ that focuses on ‘checking the boxes’ to a ‘persistence model’ that stresses more comprehensive and enduring operations.[66] This includes strategies such as (*a*) defend/hunt forward—the coordinated pre-positioning of tools in networks and systems of allies and partners to enable early engagement and discovery of threats; (*b*) ‘persistent engagement’—continuous operations that aim to intercept and halt cyber threats, and to degrade the capabilities and networks of adversaries; and (*c*) ‘limit, frustrate and disrupt’—undermining adversary activities below the threshold of armed conflict to achieve favourable security conditions.[67] Some US experts underscore the fact that, within this evolving framework, cyber risk reduction efforts must be continuous and bolstered by improved familiarity with systems under threat, particularly critical infrastructure.[68] This approach displays some similarities to Chinese views of persistence under ‘peacetime–wartime integration’ and regulatory frameworks serving ‘as means to an end rather than the end goal’, suggesting a baseline for the USA and China to engage productively on these issues.[69] Moreover, given that US and European experts have expressed concerns over Chinese and Russian APTs, and Chinese experts are preoccupied with US defend/hunt forward operations, there remain ample threat perceptions—and misperceptions—that merit further engagement on escalation and stability risks.[70]

At the multilateral level, the USA has promoted enhanced collaboration on the enforcement of existing regulations, with ransomware viewed as a primary area of cooperation, as with the Counter Ransomware Initiative that has expanded to 68 members.[71] Beyond collective efforts against ransom-

[63] US experts, Views expressed at the SIPRI workshop (note 3).

[64] US expert, View expressed at the SIPRI workshop (note 3).

[65] US experts, Views expressed at the SIPRI workshop (note 3).

[66] US experts, Views expressed at the SIPRI workshop (note 3).

[67] US Cyber Command Public Affairs Office, ‘CYBER 101—defend forward and persistent engagement’, Press release, 25 Oct. 2022; US Cyber Command Public Affairs Office, ‘Cyber 101: Hunt forward’, 960th Cyberspace Wing, 15 Nov. 2022; and US Department of Defense (DOD), *2023 Cyber Strategy: Summary* (DOD: Washington, DC, Sep. 2023).

[68] US experts, Views expressed at the SIPRI workshop (note 3).

[69] Saalman, Su and Saveleva Dovgal (note 1); and Saalman, L., Su, F. and Saveleva Dovgal, L., ‘Cyber posture trends in China, Russia, the United States and the European Union’, SIPRI, Dec. 2022.

[70] Chinese expert, View expressed at the SIPRI workshop (note 3).

[71] White House, International Counter Ransomware Initiative 2024 Joint Statement, 2 Oct. 2024.

ware, the USA aims to expand its defend/hunt forward operations to ensure greater alignment with allies and partners in undertaking early engagement and discovery of threats.[72] In terms of norm building, some US experts have advocated for building greater multilateral consensus on peacetime restraint and behaviours in cyberspace. One US expert has linked such consensus to Article 14 of the 1977 Additional Protocol II to the Geneva Conventions (Protocol II), such that states agree to not use destructive cyber operations to target core critical infrastructure 'indispensable to the survival of the civilian population'.[73] Adding to the list, the US expert noted that states could also agree to not target nuclear command, control and communications (NC3) systems through cyber operations, and to only respond to cyber aggression with non-kinetic means, such as cyber, diplomatic and economic tools.

European Union

The EU faces unique challenges in aligning its regulatory processes with implementation at the member-state level. The range of risks cited by European experts is broad and complex, and includes the use of cyberspace to compromise democracy, economy and society, with a focus on election security and hacktivism, as well as misinformation to amplify fissures and concerns over supply chain weaknesses; and cyberattacks impacting SMEs and critical infrastructure in healthcare, energy and educational sectors. Some European experts have stressed that this risk landscape means the EU needs to undertake a more proactive stance in requiring companies to adopt stricter cybersecurity and cyber risk reduction measures in accordance with EU standards.[74] These standards must also account for the GDPR by balancing privacy and cybersecurity, while placing cyber incidents and disruption into different categories of risk.[75] One European expert has advocated for a cyber risk management framework based on technical parameters rather than political measures, namely (*a*) clarifying what cyber incidents are undesirable; (*b*) mapping the chain of events likely to bring about these cyber incidents; and (*c*) locating intervention points to break this chain.[76] Such approaches recognize that a focus on 'intent' may leave out other sources of threat, since cyber incidents are often not state-driven but arise through malfunction or human error.[77]

Recognizing the need for knowledge sharing and capacity building, the EU has promoted jointly funded—by the EU and member states—initiatives targeting SMEs in the EU, incentivizing them to develop the skills and expertise necessary to bolster their cybersecurity. For example, an allocation of €30 million was proposed to support the implementation

[72] US expert, View expressed at the SIPRI workshop (note 3).

[73] US expert, View expressed at the SIPRI workshop (note 3); International Committee of the Red Cross, 'Article 14—Protection of objects indispensable to the survival of the civilian population', International Humanitarian Law Databases, [n.d.]; and Protocol II Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, opened for signature 12 Dec. 1977, entered into force 7 Dec. 1978, Art. 14.

[74] European expert, View expressed at the SIPRI workshop (note 3).

[75] European expert, View expressed at the SIPRI workshop (note 3).

[76] European expert, View expressed at the SIPRI workshop (note 3).

[77] For more information on cyber incidents driven by intent versus malfunction and human error see Saalman, L., Saveleva Dovgal, L. and Su, F., 'Mapping cyber-related missile and satellite incidents and confidence-building measures', SIPRI Insights on Peace and Security no. 2023/10, Nov. 2023.

of the NIS 2 Directive and the CRA to enhance cybersecurity in the private sector, including SMEs, across the EU.[78] In recognition of the varying threat perceptions and capabilities for addressing cyber risks at the member-state level, the EU has established a Network of National Coordination Centres, comprising 27 centres—one from each member state. This network aims to coordinate efforts and to enhance the overall cybersecurity competitiveness of the EU.[79] While the Cyber Diplomacy Toolbox seeks to harmonize the attribution process across the EU, its sanctions regime has limitations, particularly as state actors are not included in the scope.[80] Moreover, as one European expert noted, there is an imbalance of power among member states, citing the example of Germany and France having more bargaining power when it comes to public attribution and the issuance of follow-on sanctions.[81] Similarly, within the private sector, larger companies have the economies of scale to implement stringent cybersecurity requirements and regulations, while SMEs often lack these resources.[82] Accordingly, some European experts have called for greater allocation of funding and training to bolster the ability of start-ups and SMEs to meet growing cyber risk reduction requirements.

In line with US experts, some European experts emphasize the need to enhance law enforcement collaboration on such issues as ransomware. These European experts recommend enhancing knowledge sharing among governments, and attribution among like-minded nations, while building international norms and proportionate responses. One European expert noted the positive effects of public attribution as a means of norm-building and signalling, allowing for more effective communication of potential escalatory risks and redlines pertinent to an adversary's potential destructive behaviour in cyberspace.[83] Nevertheless, there are risks to such attribution and signalling if the potential response of other cyber actors is not well understood. In the context of mitigating such risks, some European experts have suggested engaging in regularized communication and dialogues on such topics as safeguards, trust and predictability, which aligns with discussion among Chinese experts of the need for greater interaction on responsibility, due diligence, accountability, and quantifying and qualifying harm.[84]

Further, one European expert expressed the need for a more substantive multilateral discussion on designations of critical infrastructure.[85] According to this view, greater clarity on critical infrastructure would elucidate Chinese concerns over data manipulation and misuse by foreign governments; Russian misgivings over the impact of using foreign software and hardware on CII operational resilience and information security; US concerns over persistent cyber operations targeting its critical infrastructure; and EU apprehension

[78] Council of the EU, 'Commission opens calls worth €107 million to strengthen Europe's cybersecurity', Press release, 25 May 2023.

[79] European Cybersecurity Competence Centre and Network, 'National Coordination Centres', [n.d.].

[80] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, *Official Journal of the European Union*, L129, 17 May 2019.

[81] European expert, View expressed at the SIPRI workshop (note 3).

[82] European expert, View expressed at the SIPRI workshop (note 3).

[83] European expert, View expressed at the SIPRI workshop (note 3).

[84] European expert, View expressed at the SIPRI workshop (note 3).

[85] European expert, View expressed at the SIPRI workshop (note 3).

over the leveraging of cyberspace to compromise democracy, economy and society through election interference, hacktivism and misinformation to amplify fissures. Some European experts emphasized building international norms, potentially beginning with attribution among like-minded actors. In this respect, the EU has expanded its use of export controls to regulate the trade in cybersurveillance tools through such mechanisms as the Wassenaar Arrangement, which added intrusion software to its dual-use list in 2013 with the aim of reducing associated risks.[86]

IV. Enhancing the EU's role

Based on the above overview of Chinese, Russian, US and EU measures and proposals to enhance cyber risk reduction, this section suggests measures that the EU could take to enhance its own role among member states and to foster collaborative engagement with China, Russia and the USA.

While the EU has made strides in coordinating efforts to reduce cyber risk, when it comes to regulations that need to be transposed into national laws, fragmentation and variations in adoption often occur at the member-state level. The various ways in which the NIS 2 Directive has been implemented under national legislation demonstrate the differences. For example, member states do not require compliance from the same sectors. As just one example, Croatia has added the education sector and the Czech Republic has added military industry to their respective lists.[87] This variation reflects differing national priorities and perceptions of risk, resulting in a patchwork of regulations across the EU. For addressing this fragmentation challenge, a collective database for tracking the implementation differences among member states regarding EU directives could (*a*) provide a clearer overview for information sharing; (*b*) ensure that stakeholders with limited capacities can keep track of regulatory frameworks; and (*c*) help foreign vendors to better understand the diverse regulatory landscape across various member states. Further, to enhance internal compliance with EU regulations relating to cyber risk reduction, member states could clarify industry-specific penalties for violations, which would contribute to strengthening approaches toward vendor management and responsibility.

The EU could also use technical parameters to strengthen its cyber risk management framework, so that member states and industries could better coordinate in preventing, detecting and responding to cyber incidents. One example is standardization of network segmentation requirements to defuse the spread of ransomware, particularly in hospitals. This could be extended to other industry and critical infrastructure sectors. Further, to strengthen the implementation of regulatory measures, the EU could (*a*) invest additional resources in ensuring common standards in the application of export control regimes that can be applied in cyberspace, such as the trade in intrusion software and other cyber surveillance tools listed under the Wassenaar Arrangement; and (*b*) expand outreach to vendors and designers of ICT products to

[86] European experts, Views expressed at the SIPRI workshop (note 3); Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies; and Bromley, M., 'Export controls and cyber-surveillance tools: Five suggestions for the Summit for Democracy', SIPRI Commentary, 8 Mar. 2024.

[87] OpenKRITIS (note 13).

foster a better understanding of their content. Such engagement between the public sector and the private sector would benefit industries in preparing for risks associated with cross-border transactions and non-state actor targeting. Capacity building could also involve EU member states sharing a short-list of regulatory and supply chain requirements to streamline reporting of cyber incidents. Further, tax incentives could be applied across member states to assist companies in purchasing cyber defense software and hardware and in undertaking cybersecurity training programmes.

The EU could also serve as a platform for facilitating multilateral exchanges on harm, signalling and escalatory risks in cyberspace. This could include everything from promoting broader membership in the Counter Ransomware Initiative to championing cyber norms, including those under Protocol II of the Geneva Convention that states will not target core critical infrastructure with destructive cyber operations. Given the risks to nuclear and other critical infrastructure, the EU facilitating or serving as a platform for such exchanges could ultimately engage countries like China, Russia and the USA. While experts from all three cyber actors are reticent to apply an arms control framework to cyberspace given obstacles to verification, they have raised examples from this field, including the need to contextualize rather than silo cybersecurity to better understand how cyber incidents and operations affect nuclear issues and strategic stability. Further, experts from China, Russia and the USA have cited the utility of joint exercises on language and vocabulary to explore similarities and differences in terminology, as the permanent members of the UN Security Council have previously done with a nuclear glossary.[88] Even at a smaller scale, the EU can facilitate engagement in these efforts with such regional organizations as the Association of Southeast Asian Nations (ASEAN) Regional Forum and the Council for Security Cooperation in the Asia-Pacific, or even with international organizations like the International Telecommunication Union.

Finally, given that international collaboration on cyber risk reduction remains fraught, the EU could develop its own risk management, public administration or policy model to serve as a framework in launching such multilateral exchanges.

V. Conclusions

Despite their economic, political and strategic differences, when it comes to cyber risk reduction, China, Russia, the USA and the EU face the same challenges in terms of terminology, data transfer and trade flows, jurisdictional tensions, and penalty enforcement. Each of the four actors has implemented or proposed various cyber risk reduction measures, some unique and some similar. These measures include (*a*) standardizing terminology and regulatory frameworks; (*b*) scaling cooperation between the public and private sectors; (*c*) strengthening vendor management and fostering cross-jurisdictional collaboration; (*d*) creating positive incentives in the form of subsidies, cyber insurance and tax codes; (*e*) integrating cyber risks into broader strategic risk dialogues; and (*f*) cooperating on cybersecurity initiatives at both regional

[88] Treaty on the Non-Proliferation of Nuclear Weapons, 2020 Review Conference of the Parties, 'P5 glossary of key nuclear terms', Working paper submitted by China, France, Russia, the United Kingdom and the United States, NPT/CONF.2020/WP.51, 31 Dec. 2021.

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.

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

SIPRI RESEARCH POLICY PAPER

ENHANCING CYBER RISK REDUCTION AND THE ROLE OF THE EUROPEAN UNION

LARISA SAVELEVA DOVGAL, FEI SU AND LORA SAALMAN

and international levels, including through fostering greater multilateral consensus on peacetime restraint and acceptable behaviours in cyberspace.

These challenges and enhancements in cyber risk reduction, informed by a previous SIPRI report and workshop featuring Chinese, Russian, US and European experts, provide opportunities to strengthen regulatory efforts. For the EU, which develops its regulations at the transnational level while leaving their implementation to member states at the national level, a key challenge is how to better align its cyber-related regulatory frameworks and initiatives with practice. Nevertheless, there are approaches the EU can adopt to enhance its role in cyber risk reduction within the EU at the transnational and member-state level, and at the international level. These include—within the EU: (*a*) clarifying sector-specific terminology and departmental responsibilities; (*b*) establishing a collective database for mapping the transposition of EU directives into national legislation; (*c*) specifying industry-specific penalties to strengthen vendor management and accountability; (*d*) strengthening its cyber risk management framework through technical parameters; (*e*) engaging in outreach with vendors and designers of ICT products to enhance understanding of relevant export control regimes; (*f*) sharing a short-list of regulatory and supply chain requirements; (*g*) leveraging tax incentives and conducting cybersecurity training across member states; and—at the international level: (*h*) championing cyber norms for critical infrastructure; (*i*) providing a platform for dialogue on terminology and cyber crossover with nuclear issues and strategic stability; (*j*) engaging with regional organizations to strengthen cyber engagement; and (*k*) developing and promoting the EU's own cyber risk management, public administration or policy model to serve as a baseline for multilateral exchanges.

These approaches will not only enable the EU to strengthen its own regulatory efforts but will also enhance the EU's role in fostering collaborative engagement on cyber risk reduction with China, Russia and the USA.

DOI: https://doi.org/10.55163/XYYF1023