SIPRI Research Policy Paper
December 2023

ADVANCING THE ROLE OF THE EUROPEAN UNION IN PROMOTING GLOBAL CYBER STABILITY

FEI SU, LARISA SAVELEVA DOVGAL AND LORA SAALMAN

SUMMARY

● While the European Union (EU) as a collective entity has not endorsed an offensive cyber posture, several of its member states have adopted both defensive and offensive activities and capabilities in cyberspace. In doing so, these member states mirror trends in China, Russia and the United States, which seem to possess increasingly similar strategies for balancing defensive and offensive cyber operations. Given this context, EU policy will need to navigate the potential involvement of its member states in offensive operations while continuing to advocate for a defence-centric strategy that emphasizes cyber resilience. This SIPRI Research Policy Paper builds on a year and a half of SIPRI research, workshops and publications that explore ways forward for the EU to strengthen its own cybersecurity while contributing to global cyber stability.

Increasing reliance on digital solutions and cross-sector interconnectivity, coupled with the emergence of transnational security threats originating from cyberspace, has prompted the European Union (EU) to respond with various initiatives for bolstering its comprehensive cyber defence strategy, aimed to 'protect, detect, defend and deter against cyberattacks'.[1] To achieve this goal, the EU has committed substantial resources to fortifying cyber stability through the introduction of new legislation on cybersecurity and cyber resilience, such as the proposed Cyber Resilience Act and the Cyber Solidarity Act, as well as amendments to existing policies and directives, including the EU Policy on Cyber Defence and the EU Network and Information Security Directive (NIS Directive).[2]

While most cyberattacks occur outside the context of armed conflicts, the war in Ukraine has demonstrated the role that offensive cyber operations may play in future battlefields, aligning with kinetic military actions. This war has posed both a challenge—with European information and communication technology (ICT) infrastructure targeted by offensive cyber operations—and a unique opportunity for the EU to refine its strategic response to offensive cyber operations during wartime. It has also focused attention on the increase in cyber operations during peacetime, which have become a standard tool of competition between states, particularly for intelligence-gathering through espionage and for conducting information campaigns such as cyber-enabled influence efforts and interference in elections.[3] Meanwhile, China, Russia and the United States appear to possess increasingly similar strategies for balancing defensive and offensive cyber operations through a constant cycle of preparation, detection, mitigation,

[1] European Commission, 'EU Policy on Cyber Defence', Joint Communication to the European Parliament and the Council, No. JOIN(2022) 49, 10 Nov. 2022, p. 2.

[2] European Commission, 'Cybersecurity policies', [n.d.]; European Commission, 'EU Policy on Cyber Defence' (note 1); and Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), *Official Journal of the European Union*, L333, 14 Dec. 2022. See also Saalman, L., Su, F. and Saveleva Dovgal, L., 'Cyber posture trends in China, Russia, the United States and the European Union', SIPRI, Dec. 2022; and Saalman, L., Su, F. and Saveleva Dovgal, L., 'Cyber crossover and its escalatory risks for Europe', SIPRI Insights on Peace and Security Paper no. 2023/9, Sep. 2023.

[3] 'Strategic competition in cyberspace: Challenges and implications—workshop summary', Center for Global Security Research, July 2019.

resilience and response.[4] As the EU navigates these complexities, a few EU member states such as Denmark, Greece, Sweden and the Netherlands have developed their own national offensive cyber capabilities.[5] Rather than limiting the definition of offensive cyber capabilities to those used during wartime, this paper defines such capabilities to include the detection of potential threats within public networks and pre-emptive disruption of cyberattacks during peacetime by 'access[ing] a computer system or network to damage or harm living or material entities'.[6] In doing so, the paper reflects the evolving trends within China, Russia and the USA towards more holistic strategies in cyberspace with growing crossover between defensive and offensive cyber operations, spanning both peacetime and wartime.[7]

The fact that the deployment of offensive cyber capabilities is a sovereign decision to be undertaken by each EU member state contributes to divided practices within the EU.[8] This is despite the EU's concerns that offensive cyber operations could contribute to a digital arms race.[9] Given this context, EU policy will therefore need to navigate the potential involvement of its member states in offensive operations while continuing to advocate for a defence-centric strategy that emphasizes cyber resilience.[10] This research policy paper builds on SIPRI workshops and publications on cyber postures, cyber incidents and related confidence-building measures of four cyber actors—China, Russia, the EU and the USA.[11] It begins by highlighting the challenges of cyber stability and the distinct approaches of these four actors. The paper then explores the potential measures the EU can employ to take direct or facilitative actions to enhance its own cybersecurity while contributing to global cyber stability. It concludes by suggesting a direction for future research.

I. Cybersecurity trends and challenges

Cybersecurity has evolved beyond its traditional focus on personal data protection and cybercrime, extending its influence across the realms of

[4] Saalman, Su and Saveleva Dovgal, 'Cyber posture trends in China, Russia, the United States and the European Union' (note 2).

[5] Jacobsen, J. T., 'Europe is developing offensive cyber capabilities. The United States should pay attention', Council on Foreign Relations Blog, 26 Apr. 2017.

[6] Brumfield, C., 'US government offensive cybersecurity actions tied to defensive demands', *CSO*, 12 Sep. 2022; and Smeets, M., 'A matter of time: On the transitory nature of cyberweapons', *Journal of Strategic Studies*, vol. 41, nos 1–2 (2018).

[7] Saalman, Su and Saveleva Dovgal, 'Cyber posture trends in China, Russia, the United States and the European Union' (note 2).

[8] Bendiek, A. and Bund, J., 'Shifting paradigms in Europe's approach to cyber defence', Stiftung Wissenschaft und Politik (SWP) Comment No. 48, 25 Sep. 2023.

[9] Weber, V., 'Rethinking European cyber defense policy', German Council on Foreign Relations (DGAP) Policy Brief, 1 Apr. 2022.

[10] Saalman, Su and Saveleva Dovgal, 'Cyber posture trends in China, Russia, the United States and the European Union' (note 2); and Bendiek and Bund (note 8).

[11] Saalman, Su and Saveleva Dovgal, 'Cyber posture trends in China, Russia, the United States and the European Union' (note 2); Saalman, Su and Saveleva Dovgal, 'Cyber crossover and its escalatory risks for Europe' (note 2); Saalman, L., Su, F. and Saveleva Dovgal, L., 'Mapping cyber-related missile and satellite incidents and confidence-building measures', SIPRI Insights on Peace and Security no. 2023/10, Nov. 2023; 'Cyber incidents and threat perceptions: Views from China, Russia, Europe and the United States', SIPRI workshop, Stockholm, 13–14 June 2023; and 'Cyber postures and dynamics: China, Russia, United States and Europe', SIPRI and the Observer Research Foundation America workshop, Washington, DC, 2–3 Nov. 2022.

politics, economics and national security. Policymakers are increasingly focused on cybersecurity, but there are still challenges in determining the best governance approaches for cyberspace. The multifaceted, evolving and global nature of cyber threats demands coordinated responses that incorporate multiple stakeholders and partnerships, both with like-minded nations and potential adversaries. The relative absence of consensus on cyber norms among the major cyber actors, namely China, Russia, the EU and the USA, including their respective positions in United Nations forums at various levels, poses a significant challenge to advancing global cyber stability. The lack of a common official definition of cyber stability is a further complication. Nevertheless, in 2019 the Global Commission on the Stability of Cyberspace—a multistakeholder forum supported by governments, public organizations and private industry—defined stability of cyberspace as: 'everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner.'[12] Based on this definition, this section highlights the challenges for cyber stability and the distinct approaches to cybersecurity of China, Russia, the EU and the USA, in the context of trends of intensifying cyber operations that have been exacerbated by recent international developments.

Growing complexities in characterizing cyber behaviour

Unlike cyber operations conducted in the context of the war in Ukraine, which are part of military operations, the characterization of cyber operations during peacetime remains less clear in terms of what should be regarded as defensive or offensive. For example, US officials describe 'hunt forward' operations—in which US military cyber experts are deployed to a foreign nation to detect malicious activity on the host nation's networks—as 'strictly defensive' and carried out 'at the request of partner nations'.[13] However, China and Russia see things differently. China regards them as cyber operations with an offensive nature that infringe the sovereignty of other nations' networks.[14] Likewise, Russian officials have taken a highly critical stance against these 'forward cyber operations', classifying them as 'cyber aggression'.[15] While cyber espionage for intelligence-gathering purposes is widely practised, any tangible impacts of such operations—in particular the mass targeting of supply chains or critical infrastructure that compromises vital societal functions and national security—could fundamentally escalate

[12] Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, Final Report, Nov. 2019, p. 13.

[13] US Cyber Command, 'CYBER 101: Hunt forward operations', News, 15 Nov. 2022.

[14] Tang L., '从网络空间军事行动新态势看网络安全的重要性' [The importance of network security from the new situation in cyberspace military actions], 人民论坛 • 学术前沿 [*People's Tribute*], 18 Aug. 2021; and China Electronics Technology Group Corporation, 30th Research Institute, '解析美军 "前出狩猎" 网络行动' [Analysis of the US military's 'hunt forward' cyber operations], *Information Technology and Network Security*, 17 May 2023.

[15] 'МИД обвинил США в проведении кибератак против России руками Украины' [The Foreign Ministry accused the United States of carrying out cyberattacks against Russia at the hands of Ukraine], RBC, 25 Oct. 2022.

Table 1. Critical infrastructure sectors as defined in China, Russia, the European Union and the United States

Category	China	Russia	European Union	United States
Communications	Public communication and information services	Communications	Digital infrastructure Digital providers Information and communications technology service management	Communications Information technology
Energy	Energy	Energy Nuclear energy Fuel and energy	Energy	Energy Nuclear reactors, materials and waste
Finance	Finance	Banking and other financial services	Banking Financial market infrastructures	Financial services
Transport	Transport	Transport	Transport	Transportation systems
Chemical		Chemical	Manufacture, production and distribution of chemicals	Chemical
Defence	National defence	Defence industry		Defence industrial base
Food			Production, processing and distribution of food	Food and agriculture
Government	E-government services Public services		Public administration	Government facilities
Health		Healthcare	Health	Healthcare and public health
Manufacturing		Metallurgy Mining industry	Manufacturing	Critical manufacturing
Space		Space and rocket industry	Space	
Water	Water		Drinking water Waste water	Water & waste water systems Dams
Other	Any other important network facilities or information systems that may seriously harm national security, the national economy and people's livelihoods, or public interest in the event of incapacitation, damage, or data leaks.	Science	Research Postal and courier services Waste management	Commercial facilities[a] Emergency services

[a] Commercial facilities are defined as 'a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging'. US Cybersecurity and Infrastructure Security Agency, 'Commercial facilities sector', [n.d.].

Sources: Chinese State Council, '关键信息基础设施安全保护条例' [Regulations on the Security and Protection of Critical Information Infrastructure]', 17 Aug. 2021; Legislative Acts of the Russian Federation, 'Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"' [Federal Law of 26.07.2018 No. 187 'On the security of critical information infrastructure of the Russian Federation'], 26 July 2017; Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Official Journal of the European Union, L333, 14 Dec. 2022; and US Cybersecurity and Infrastructure Security Agency, 'Critical infrastructure sectors', [n.d.].

their consequences.[16] One potentially escalatory example is the targeting

[16] Lin, H. S., 'Offensive cyber operations and the use of force', *Journal of National Security Law & Policy*, vol 4 (2010); and Borghard, E. and Lonergan, S., 'Confidence building measures for the cyber domain', *Strategic Studies Quarterly*, vol. 12, no. 3 (Fall 2018).

through ShadowPad malware—allegedly used by China-linked groups for cyber espionage purposes—of the Indian power distribution system near a disputed border at which India and China remain engaged in a military stand-off.[17]

Beyond China, Russia and the USA, an increasing number of countries have also developed offensive cyber capabilities. These include EU member states such as Denmark, Greece, Sweden and the Netherlands, as well as other countries such as Australia, Iran, Israel, North Korea and the United Kingdom.[18] Since 2018 Germany has been developing 'active cyber defense' capabilities both for offensive and defensive purposes.[19] These developments present a challenge in establishing a benchmark for responsible state behaviour concerning the possession and use of offensive cyber capabilities. Experts from China, Russia, the EU and the USA have indicated that there is still a lack of clear domestic understanding and consensus within their own countries regarding cyber norms on acceptable and unacceptable state conduct.[20] Potentially, over time, interactions among like-minded partners and with potential adversaries may lead to a convergence of behaviours and precedents that can serve as a foundation for building global norms.[21]

Expanding definitions of critical infrastructure in cybersecurity

In the 1990s the USA established its National Infrastructure Protection Center to address the challenge of protecting critical infrastructure from threats, including those emanating from the cyber domain.[22] More specifically, in 2010, when discussing destructive cyber espionage operations, a former director of the US National Security Agency, General (Retd) Michael Hayden, raised the idea of 'forming the cyber equivalent of demilitarized zones for sensitive networks, such as the power grid and financial networks, that would be off-limits to attack from nation states'.[23] In recent years, China, Russia, the EU and the USA have each released an extensive critical infrastructure list (see table 1).

The primary goal behind such lists is to enhance the resilience of network and information systems against cybersecurity risks in the designated sectors. Russian legislation on critical information infrastructure (CII) not only lists CII entities, but also further categorizes them according to their significance to Russia's social, political, economic, ecological and national security interests. While China has designated the fewest number of sectors

[17] Council on Foreign Relations, 'Targeting of the Indian power grid', Cyber Operations Tracker, Apr. 2022; and 'Power grid of Asian nation shows signs of intrusion by espionage group', *The Record*, 12 Sep. 2023.

[18] Jacobsen (note 5).

[19] Herpig, S., 'As Germany moves toward a more offensive posture in cyberspace, it will need a vulnerability equities process', Council on Foreign Relations Blog, 4 Sep. 2018.

[20] Views of cybersecurity experts from China, Russia, the EU and the USA expressed at the 'Cyber incidents and threat perceptions: Views from China, Russia, Europe and the United States' workshop (note 11).

[21] Fischerkeller, M. and Harknett, R., 'Persistent engagement and tacit bargaining: A path toward constructing norms in cyberspace', *Lawfare*, 9 Nov. 2018.

[22] Vatis, M., Statement to the US Senate Judiciary Subcommittee on Terrorism, Technology and Government Information, 10 June 1998.

[23] Zetter, K., 'Former NSA director: Countries spewing cyberattacks should be held responsible', *Wired*, 29 July 2010.

as critical, its classification of 'other sectors' remains vague, allowing for potential expansion to include any sector based on specific circumstances.

By contrast, the EU has provided the most comprehensive list of critical sectors, particularly following the December 2022 update to the NIS Directive, which expanded the number of sectors from 7 to 18. Among these, 11 sectors listed in table 1 constitute 'sectors of high criticality', while the remaining sectors fall into the category of 'other critical sectors'.[24] The USA has gone a step further by designating all 16 sectors as 'off-limits' to destructive cyberattacks.[25]

The lists of critical infrastructure defined by these four actors reflect the multifaceted nature of cyber threats and reveal some areas of crossover, including information and communication services, energy, transportation and finance. However, their expansiveness also raises two concerns that are potentially significant. First, if all sectors are designated as critical, then the concept of criticality loses its meaning. Second, a list of infrastructure that is truly off-limits to cyberattacks could be used as a template for what to attack. Nevertheless, these common areas of concern suggest a foundational baseline that could form a collaborative starting point for all four stakeholders.

Growing public–private partnerships in cyber operations

While the discussion on private–public partnerships (PPPs) in cyberspace is not new, the increased attention to such relationships in light of the ongoing war in Ukraine presents a unique opportunity for both the private and public sectors to prioritize collaborative efforts. As highlighted by the prime minister of Estonia, Kaja Kallas, 'the private sector has transformed its role during this war, and taken public–private partnership up a level in defense of digital infrastructure'.[26] There is a growing need to transition from mere event-based responses, such as Microsoft's technical support and humanitarian assistance to Ukraine,[27] to the establishment of a sustainable, long-term framework for private sectors' engagement in cyber incident response and cyber defence. Meanwhile, it is also important to acknowledge the lack of regulation governing the extent to which the private sector may engage in offensive cyber operations, even when at the official request of a government. An illustration is Ukraine's call to form an IT Army of volunteers and its offensive cyber operations against targets in Russia.[28]

The April 2023 EU Cyber Solidarity Act proposes an EU Cybersecurity Reserve, which will consist of trusted and certified providers from the private sector that would be ready to intervene in cyber incidents at the request of member states.[29] The USA has also actively advocated the

[24] Directive (note 2).

[25] Soldatkin, V. and Pamuk, H., 'Biden tells Putin certain cyberattacks should be "off-limits"', Reuters, 17 June 2021.

[26] 'Kaja Kallas says Ukraine is giving the free world a masterclass on cyber-defence', *The Economist*, 17 Apr. 2023.

[27] Smith, B., 'Extending our vital technology support for Ukraine', Microsoft On the Issues Blog, 3 Nov. 2022.

[28] Render-Katolik, A., 'The IT Army of Ukraine', Center for Strategic and International Studies, 15 Aug. 2023.

[29] European Commission, 'Cybersecurity policies' (note 2); European Commission, 'The EU Cyber Solidarity Act', 20 June 2023; and Cyber Risk, 'The EU Cyber Solidarity Act', 2023.

importance of PPPs in defending its cyberspace. This emphasis is clearly outlined in both its March 2023 US National Cybersecurity Strategy and its September 2023 US Cyber Strategy of the Department of Defense (DOD Cyber Strategy).[30] Aligning with these strategies, the US Cybersecurity and Infrastructure Security Agency (CISA) issued a Cybersecurity Strategic Plan which lays out several objectives for the 2024–26 financial years relevant to PPPs, such as enhancing visibility into, and ability to mitigate cybersecurity threats and campaigns; identifying and mitigating critical and exploitable vulnerabilities, as well as fostering joint cyber defence operations; and coordinating responses to significant cybersecurity incidents, among others.[31]

In China, collaboration between the private and public sectors is notably close in respect to cybersecurity. Qihoo 360, a prominent private cybersecurity company in China, has been actively assisting government, military, scientific research and financial sectors since 2011 in identifying and defending against cyber espionage operations.[32] Further, other cybersecurity companies, such as Datacloak, Qi An Xin, Threatbook, Chaitin Tech, Trusfort and others, collaborate closely with state institutions as well as large Chinese telecommunication companies on domestic software and hardware solutions to enhance national cybersecurity.[33] This reflects an enhanced sense of national duty in relation to China's cyber defences, in that many of its cybersecurity companies, despite being privately owned, label themselves as de facto 'national teams' dedicated to defending the country against cyberattacks.[34] This sense of national duty, however, is also notably underscored by legal obligations and protections. For example, Article 7 of the 2017 National Intelligence Law states: 'All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of. The State protects individuals and organizations that support, assist, and cooperate with national intelligence efforts.'[35] It is also worth noting that government recognition is crucial for companies operating in China to secure financial support, particularly within the domestic market.

In Russia, the development of PPPs to address cybersecurity challenges has been driven by both domestic legal concerns and international events, including the ongoing war in Ukraine. National legislation allowing PPPs on information technology (IT) solutions entered into force in 2018.[36] In 2022, as the war in Ukraine unfolded with cyberattacks also targeting Russia's critical

[30] White House, *National Cybersecurity Strategy* (White House: Washington, DC, 1 Mar. 2023); and US Department of Defense (DOD), *Summary: 2023 Cyber Strategy of the Department of Defense* (DOD: Washington, DC, 12 Sep. 2023).

[31] US Cybersecurity and Infrastructure Security Agency (CISA), *CISA Cybersecurity Strategic Plan, FY2024–2026* (CISA: Sep. 2023).

[32] Qihoo 360, '奇虎360大事记' [Qihoo360 major events], [n.d.], (in Chinese).

[33] Threat.Technology, 'These are the top cyber security companies in China (2021)', [n.d.].

[34] '奇安信首次盈利，网络安全国家队将迎来收获期?' [Qi'anxin makes profit for the first time, will the national network security team usher in a harvest period?], 36KR, 1 Feb. 2023; and Qihoo 360 major events (note 32).

[35] 'PRC National Intelligence Law (as amended in 2018)', China Law Translate, 27 June 2017.

[36] Legislative Acts of the Russian Federation, 'Федеральный закон от 29.06.2018 г. № 173-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации"' [Federal Law of 29.06.2018 No. 173 'On amendments to certain legislative acts of the Russian Federation'], 29 June 2018.

sectors, the Russian Ministry of Digital Development, Communications and Mass Media (Минцифры) proposed a draft bill on 'white hat hackers', also known as 'ethical hackers', who would test for and identify security vulnerabilities in hardware, software or networks.[37] In February 2023, in collaboration with Russian cybersecurity companies, the Ministry launched its first bug bounty programme to test the infrastructure of Russia's Public Services Portal (Госуслуги) and is planning to expand the scope to also search for vulnerabilities in national biometric and identification and authentication systems before the end of 2023.[38] In November 2023, Russia's Big Data Association (RUBDA)—a group of the largest Russian IT companies, both privately and publicly owned—drafted the Industry Standard for Data Protection Concept that defines reliable approaches to storing and collecting data as well as methods for improving information security.[39] Notably, during the high-level week of the 78th session of the UN General Assembly in 2023, to celebrate the 25th anniversary of the international information security agenda at the UN, the Russian deputy foreign minister held an informal meeting with representatives of the UN secretary-general and partner organizations, as well as representatives of Solar—Russia's publicly owned IT company.[40] Thus, while being reluctant to include non-state actors in state-level cyber discussions, Russia nevertheless seems to recognize the benefits of IT company participation.

Increasing focus on state-of-the-art technologies in cybersecurity

As the number and sophistication of cyberattacks continue to increase, the EU has recognized the need to make use of 'cutting edge technologies' to gain an advantage over competitors and adversaries.[41] These technologies include artificial intelligence (AI), big data and quantum computing.[42] The development of a European Cybersecurity Shield under the EU Solidarity Act includes the deployment of cutting-edge technologies to monitor, identify and share timely warnings on cyber threats.[43] Moreover, the 2022 EU Cyber Defence Policy proposes a technology roadmap to identify critical cyber technologies for long-term security and defence and to reduce strategic dependencies.[44] The roadmap is part of the EU's broader efforts to boost research, technology development and innovation, while reducing

[37] 'Законопроект о белых хакерах вызвал вопросы у силовиков' [The bill on white-hat hackers raised questions among security officials], *Vedomosti*, 26 Mar. 2023.

[38] 'Взлом на благо государства: Минцифры протестирует свои сервисы белыми хакерами' [Hacking for the benefit of the state: The Ministry of Digital Development will test its services with white hackers]', *Kommersant*, 9 Nov. 2023.

[39] 'Российские IT-компании разработали концепцию отраслевого стандарта защиты данных' [Russian IT companies have developed the concept of an industry standard for data protection], Big Data Association, 3 Nov. 2023.

[40] Министерство иностранных дел Российской Федерации [The Ministry of Foreign Affairs of the Russian Federation], 'О мероприятии по международной информационной безопасности «на полях» 78-й сессии Генеральной Ассамблеи ООН' [On international information security event 'on the sidelines' of the 78th session of the UN General Assembly], Press release, 25 Sep. 2023.

[41] European Commission, 'EU Policy on Cyber Defence' (note 1), p. 1.

[42] Council of the European Union, 'Council conclusions on the development of the European Union's cyber posture', Doc no. 9364/22, 23 May 2022, Annex, para. 7.

[43] European Commission, 'The EU Cyber Solidarity Act' (note 29).

[44] European Commission, 'Cybersecurity policies' (note 2); and European Commission, 'EU Policy on Cyber Defence' (note 1), pp. 14–16.

dependencies on critical technologies and value chains for security and defence.[45] These policies reflect deep concern held by 'European stakeholders from the private and public sector as well as civil society' over the EU's dependency on foreign-owned technology providers and weak indigenous industrial capabilities.[46] More recently, the EU published a list of 10 critical technology areas that require further risk assessment, with AI and quantum technologies being among those identified as priorities.[47]

The USA also has taken a proactive approach in applying emerging technologies in cyberspace, particularly advanced predictive analytics, AI, machine learning and 5G cellular networks and low earth orbit satellites in pursuit of improved security in cyberspace. These initiatives are aimed at mitigating cybersecurity risks and remaining 'competitive in a rapidly changing digital environment'.[48] Additionally, the US Cyber Command has been working on a five-year roadmap for AI and its application in cyber operations.[49] At the Black Hat USA Conference in August 2023, the Biden administration announced the launch of an AI Cyber Challenge to be led by the Defense Advanced Research Projects Agency (DARPA). This two-year competition challenges competitors to use AI to identify and address software vulnerabilities, with the aim of creating new technologies to improve cybersecurity. Leading AI companies, including Anthropic, Google, Microsoft and OpenAI, will lend their expertise and make 'their cutting-edge technology available' in collaborating with DARPA on this initiative.[50]

Following China's launch in 2015 of the 'Internet+' initiative, a concept and strategy that seeks to apply IT in conventional industries, the country has been actively advocating the integration of AI into cyberspace.[51] Chinese policy experts have engaged in discussions about the various potential applications of AI in cyberspace, including enhancing capability to defend against cyberattacks, concealing network vulnerabilities while simultaneously identifying weaknesses in adversary networks, and advancing offensive cyber capabilities.[52] For example, Qihoo 360 has utilized AI in big data analytics for automated analysis, screening and correlation

[45] Council of the European Union, *A Strategic Compass for Security and Defence* (European External Action Service: Brussels, Oct. 2021), p. 47.

[46] Sahin, K. and Barker, T., *Europe's Capacity to Act in the Global Tech Race: Charting a Path for Europe in Times of Major Technical Disruption*, German Council on Foreign Relations (DGAP) Report No. 6, 22 Apr. 2021, p. 2.

[47] European Commission, 'Commission Recommendation of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States', C(2023) 6689, 3 Oct. 2023, p. 3 and Annex.

[48] Jones, K. A., 'Modernizing cybersecurity in US diplomatic technology: Our global call to action', Keynote remarks of the US Department of State's chief information officer, Security Transition Summit, 2 Dec. 2021.

[49] National Security Agency, 'GEN Nakasone offers insight into future of cybersecurity and SIGINT', 21 Sep. 2023.

[50] White House, 'Biden–Harris administration launches artificial intelligence cyber challenge to protect America's critical software', Briefing Room statement, 9 Aug. 2023.

[51] Chinese State Council, '国务院关于积极推进 "互联网+" 行动的指导意见' [Guiding opinions of the State Council on actively promoting the 'Internet+' action], 4 July 2015.

[52] 罗曦 [Luo X.], '人工智能技术可能加剧核战争风险' [Artificial intelligence technology may increase the risk of nuclear war], 世界知识 [*World Affairs*], no. 16 (2019), pp. 68–69; and 韩洪涛 [Han H.], '人工智能在核作战体系中的潜在应用及影响浅析' [Analysis of the potential application and impact of artificial intelligence in the nuclear warfare system], 国防科技 [*National Defence Technology*] vol. 43, no. 4 (Aug. 2022), p. 80.

of massive samples to discover cyberattack clues.[53] In contrast to the EU and the USA, China rarely specifies in official doctrines its detailed plans and ambitions for applying AI and other emerging technologies to advance cybersecurity. Instead, China has issued several regulations with a primary focus on ensuring information security and strengthening content control, such as the 2021 Regulations on Algorithm Recommendation Management in Internet Information Service, the 2022 Regulations on Deep Synthesis in Internet Information Services, and the 2023 Regulation on Generative AI.[54] Nevertheless, China recognizes the potential opportunities that AI offers in enhancing its cybersecurity alongside the increasing complexities it poses in cybersecurity governance.

Russia has achieved more modest results regarding the development of civilian AI capabilities and their application for cybersecurity. Russia's first national strategy on the development of AI was adopted in 2019, with a particular focus on economic and social benefits of implementing AI as well as its advantages for enhancing national security.[55] Nevertheless, Russian cybersecurity companies have acknowledged the potential of AI to reinforce cybersecurity and have succeeded in developing several AI-based solutions, including the automated detection and prevention of both known and unknown cyberattacks, and the use of multiple machine learning techniques in user behaviour analytics.[56]

II. Recommendations

Building upon the preceding trends, this section explores the potential direct or facilitative actions the EU can take to enhance global cyber stability.

Deepen discussion of acceptable and unacceptable cyber behaviour

The UN norms of responsible state behaviour in cyberspace, set out in the 2015 report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security, comprise 11 voluntary, non-binding rules.[57] Within these rules, three are prohibitive (i.e. actions that should not be taken), while the remainder outline positive obligations (i.e. actions that are advisable to

[53] Qihoo 360, '三六零安全科技股份有限公司2022 年年度报告' [*Qihoo 360 2022 Annual Report*], 20 Apr. 2023, (in Chinese).

[54] Cyberspace Administration of China, '互联网信息服务算法推荐管理规定' [Regulation on Algorithm Recommendation Management in Internet Information Service], 31 Dec. 2021; Cyberspace Administration of China, '互联网信息服务深度合成管理规定' [Regulation on Deep Synthesis in Internet Information Services], 25 Nov. 2022; and Cyberspace Administration of China, '生成式人工智能服务管理暂行办法' [Regulation on Generative AI], 13 July 2023.

[55] 'Указ Президента Российской Федерации от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации"' [Presidential Decree of 10.10.2019 No. 490 'On the development of artificial intelligence in the Russian Federation'], Legislative Acts of the Russian Federation, 10 Oct. 2019.

[56] 'Искусственный интеллект внедряется в кибербезопасность' [Artificial intelligence is being introduced into cybersecurity], Expert.ru, 24 Apr. 2023.

[57] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report, A70/174, 22 July 2015, para. 13.

pursue).[58] Despite being a step towards establishing responsible behaviour in cyberspace, the UN norms have limitations in enabling member states—which include China, Russia, the EU and the USA—to assess the boundaries of cyber operations and understand how these actions are perceived by adversaries. These constraints are problematic in preventing or mitigating an escalatory scenario, particularly in the current unpredictable geopolitical environment. Deepened bilateral and multilateral exchanges of what are perceived as acceptable and unacceptable cyber behaviours are therefore urgently needed. One promising multilateral platform is the International Counter Ransomware Initiative. Launched in 2021, this multilateral effort has expanded to include 50 member states. One of its primary focal points is fostering an understanding of responsible state behaviour.[59]

Moreover, the EU could facilitate bilateral or trilateral information exchanges with China and the USA. However, given the ongoing conflict in Ukraine, such exchanges with Russia are unlikely. Instead, the EU could possibly engage with Russia through a track-2 (non-governmental dialogue) process organized by a neutral party. Moreover, amidst the prevailing trend in China, Russia and the USA to pursue offensive cyber capabilities, the EU stands apart with a preference for a defence-centric approach. This distinctive stance provides the EU with an opportunity to champion the development of a framework aimed at addressing the challenges that may emerge as offensive cyber capabilities continue to evolve and proliferate. It also grants the EU a neutral status for facilitating exchanges, positioning it as a less confrontational party.

To achieve this at the international level, however, requires establishing a shared baseline within the EU. The 27 member states' respective perceptions of risks and challenges diverge widely, as do their national cyber capabilities, resulting in various levels of preparedness for responding to cyberattacks and different interpretations regarding escalation thresholds. These differences hinder not only the overall cyber stability within the bloc but also impede the efforts of the EU and its member states to articulate a cohesive position on how to respond effectively and engage with other cyber powers, especially with regard to cyber norms. To enhance the overall competence of all its member states, the EU has established a Network of National Coordination Centres. As of October 2023, 25 national centres are listed in this network.[60]

Identify off-limits critical infrastructure

Cyberattacks against dual-use infrastructure—that is, infrastructure used both for civilian and military purposes, such as satellite services—have the potential to escalate conflicts. However, the broad and at times vague range of critical infrastructure identified by China, Russia, the EU and the USA

[58] Hogeveen, B., *The UN Norms of Responsible State Behaviour in Cyberspace: Guidance on Implementation for Member States of ASEAN* (Australian Strategic Policy Institute, International Cyber Policy Centre: Canberra, 22 Mar. 2022).

[59] White House, 'International Counter Ransomware Initiative 2023 joint statement', 1 Nov. 2023.

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

(see table 1) poses challenges in comprehending the potential escalation risks associated with targeting this infrastructure.

As a potential starting point, track-2 level discussions over cyberattacks triggering false missile alarms or targeting of satellite infrastructure provides one area in which China, Russia, the EU and the USA all share common concerns.[61] However, the differences in how each of these actors delineate civilian versus military infrastructure merits greater interaction to mitigate future escalation. Given Russian statements that 'quasi-civilian' infrastructure may become a valid target for retaliation, it is crucial to enhance understanding regarding varying interpretations on whether dual-use infrastructure constitutes a legitimate target for initiating attack or retaliation.[62]

Further, the increasing trend of cyberattacks involving cybercrime tactics used for cyberwarfare objectives also needs to be factored into EU thinking on how to respond to such operations against EU's dual-use infrastructure.[63] In contrast to equivalent policy and law in China, Russia, and the USA, the EU's December 2022 update to its NIS Directive contains fewer elements related to national security and defence, as these areas fall under the sovereignty of its member states. Consensus is needed among EU member states on whether there is a need to identify dual-use infrastructure that is off-limits and more importantly to outline the escalatory risks associated with such attacks.

Employ deconfliction lines and official cyber dialogues

The current geopolitical landscape—characterized by complex bilateral and multilateral relations between major powers such as China, the EU, Russia and the USA—poses significant challenges when attempting to work collectively on cyber-related issues. However, it is precisely these challenges that necessitate dialogue to alleviate potential misunderstandings. At the bilateral level, the first China–EU Digital Dialogue took place in September 2020 and involved discussion of cybersecurity and disinformation. Nevertheless, this dialogue was paused in July 2021 following EU condemnation of malicious cyber activities originating from within Chinese territory.[64] Fortunately, both sides have signalled their intent to resume the dialogue.[65]

In September 2021 Russian deputy foreign minister Sergei Ryabkov suggested broadening the scope of the bilateral US–Russian dialogue on cyber issues to include substantive discussions on how to prevent malicious cyber activities against each country's military control systems.[66] And in December 2021 the Russian foreign ministry extended an invitation to the EU to

[61] Saalman, Su and Saveleva Dovgal, 'Mapping cyber-related missile and satellite incidents and confidence-building measures' (note 11).

[62] Vorontsov, K. V., Statement at the second session of the openended working group on reducing space threats through norms, rules and principles of responsible behaviours, Geneva, 12 Sep. 2022, p. 2.

[63] Saalman, Su and Saveleva Dovgal, 'Cyber crossover and its escalatory risks for Europe' (note 2).

[64] Council of the EU, 'Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory', 19 July 2021.

[65] European Council, 'EU–China summit via video conference, 1 April 2022', 1 Apr. 2022.

[66] Рябков, С. [Ryabkov, S.], 'Само наше существование становится в их восприятии источником тревоги по поводу безусловного характера американского доминирования в мире' [Our very

hold collective consultations on cybersecurity, drawing on earlier bilateral interactions of Russia with France, Germany and the Netherlands.[67] While most track-1 (governmental) level dialogues between the EU and Russia have been severed due to the ongoing war in Ukraine, confidential 'deconfliction lines'—military-to-military contacts to reduce risk of miscalculation—between individual member states and Russia remain of substantial value. These deconfliction lines could also provide a way to communicate shared European concerns over cybersecurity.[68]

While some of these channels between the EU and China as well as Russia have stagnated, the USA–EU Cyber Dialogue was held in December 2022. These talks revolved around a shared commitment to a 'resilient cybersecurity partnership' and included information exchanges on their respective cyber policy frameworks.[69] Such engagement could be expanded to include greater discussion of the role of the private sector and non-state actors more broadly.

In April 2023 China and Russia held official consultations on international information security, reiterating their commitment to 'improve international legal principles in the field of application of ICT' through enhanced trust and dialogue and 'in close cooperation with developing countries'.[70] Such track-1 level exchanges, whether between partners or adversaries, are critical to sharing concerns and intentions as a means of reducing misunderstanding. A recent example is the working-level meeting between the defence officials of China and the USA, held just after the release of the September 2023 DOD Cyber Strategy, to discuss an unclassified summary of the strategy and related cyber issues.[71] The EU could pursue similar attempts to compartmentalize cybersecurity as an area where all sides hold shared interests despite intensified strategic competition.

Expand technological coverage of unofficial cyber dialogues

The proliferation of emerging technologies such as AI, advanced data analytics and quantum computing, have led to a growing impetus to expand the technological footprint of track-2 level and track-1.5 level (non-governmental and governmental) talks on cybersecurity.[72] Participation in these discussions by a range of industry, technical, military, political, academic and other experts would allow for a more multifaceted exploration of granular trends in cybersecurity. Alongside EU efforts to boost technological research and development, a separate platform could be launched for not only iden-

existence becomes, in their perception a source of anxiety about the unconditional nature of American dominance in the world], Russian International Affairs Council, 19 Aug. 2021.

[67] 'Russia proposes holding collective cybersecurity talks with EU—TASS', Reuters, 16 Dec. 2021.

[68] French Senate Committee on Foreign Affairs, Defense and Forces Armed Forces and Russian International Affairs Committee of the Federation Council, Joint report a trust agenda between France and Russia, June 2020, p. 16 (in French).

[69] US Department of State, 'The 2022 US–EU Cyber Dialogue', Media note, 21 Dec. 2022.

[70] Russian Ministry of Foreign Affairs, 'О российско-китайских консультациях по международной информационной безопасности (МИБ)' [On Sino-Russian consultations on international information security (IIS)], 19 Apr. 2023.

[71] US Department of Defense, 'US and PRC hold working level meeting on 2023 DOD Cyber Strategy Unclassified Summary and related cyber issues', Press release, 22 Sep. 2023.

[72] Malwarebytes, 'AI in cyber security: Risks of AI', [n.d.]; and Saalman, Su and Saveleva Dovgal, 'Mapping cyber-related missile and satellite incidents and confidence-building measures' (note 11).

tifying existing risks to cybersecurity, but also anticipating the emergence of new malware vectors before malicious actors can exploit them. Since the concern about striking the right balance between innovation and security is shared by different stakeholders, Chinese, Russian, EU and US technical discussions—with either no or limited official representation—could be an appropriate framework for addressing common concerns.[73]

Moreover, in areas where official discussions have been severed or are lacking, such discussions can be invaluable for keeping channels of communication open and exploring the intersection of domains of cyber threat. These talks, which can include retired military and official participants, have the advantage of exploring issues deemed overly technical or sensitive, or not yet ripe for track-1 diplomacy. Among these are the intersection of cyberspace and other domains like nuclear and space, as well as the growing impact of emerging technologies. For example, the Nuclear Threat Initiative and the Institute for US and Canadian Studies of the Russian Academy of Sciences have co-convened dialogues among US and Russian experts in cybersecurity, information security and nuclear weapons policy under the 'common understanding that nuclear weapons systems must be protected from escalating cyber threats'.[74] Further, the US National Academy of Sciences through the Center for International Security and Cooperation has conducted talks with both retired and active officials from Russia since 1980, China since 1988 and India since 1998, on nuclear, cyber, AI and a range of related issues.[75] Initiation of similar sets of track-2 and track-1.5 level dialogues facilitated by policy research institutes and involving retired military and other officials could better integrate the space and cyber domains, particularly in the wake of recent cases of satellite interference and cyberattacks.[76]

Clarify the role of the private sector in offensive cyber operations

While the war in Ukraine has galvanized collaborative efforts between the private and public sectors to enhance cyber defence of critical infrastructure, it has also highlighted the urgent need for more in-depth discussions of the implications of this collaboration. Recent policies in both the EU and the USA increasingly shift responsibility and liability to the private sector, urging private entities to secure their networks.[77] However, this approach raises concerns and risks regarding the private sector's potential engagement in 'hack-back' tactics and other offensive cyber activities without proper

[73] European Union Agency for Cybersecurity, 'Is secure and trusted AI possible? The EU leads the way', Press release, 7 June 2023.

[74] Stoutland, P., 'US–Russia Cyber–Nuclear Weapons Dialogue', Nuclear Threat Initiative, [n.d.].

[75] National Academy of Sciences, 'CISAC Security Dialogues', [n.d.].

[76] Von der Leyen, U., European Commission President, Keynote address, Tallinn Digital Summit, 10 Oct. 2022; Raju, N. and Saalman, L., 'Space and cyberspace', in *SIPRI Yearbook 2023: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2023); Saalman, Su and Saveleva Dovgal, 'Cyber crossover and its escalatory risks for Europe' (note 2); and Saalman, Su and Saveleva Dovgal, 'Mapping cyber-related missile and satellite incidents and confidence-building measures' (note 11).

[77] Saalman, Su and Saveleva Dovgal, 'Cyber crossover and its escalatory risks for Europe' (note 2), p 22.

state authorization.[78] Within the EU, member states have varying views on offensive cyber operations, and the involvement of the private sector adds to the complexity of this landscape.

The situation becomes more problematic when the private sector contributes to an ongoing armed conflict through digital tools.[79] In the context of the war in Ukraine, for example, there is an urgent need to raise awareness not only among private companies, but also among their employees, volunteers and hacktivists—such as those involved in the IT Army of Ukraine—regarding the potential of losing protection under international humanitarian law.[80] This also raises the issue of state obligations when potentially escalatory activities are undertaken by non-state actors purportedly on behalf of a government.[81] Given that the current EU Policy on Cyber Defence only contains three brief references to the role of non-state actors, this is one policy area in which the EU needs to develop more robust regulatory approaches.[82] Policy research institutes can play a crucial role by conducting comparative studies of regulatory processes in other countries and by examining the ongoing debates within international organizations like the International Committee of the Red Cross (ICRC). The October 2023 ICRC Global Advisory Board on Digital Threats during Armed Conflicts report, which examined state obligations for restraining civilian hackers during wartime called for states 'to adopt and enforce national laws that regulate civilian hacking'.[83]

III. Conclusions

The EU, as a whole, continues to refrain from adopting policies that support offensive cyber capabilities, while several of its member states have maintained both defensive and offensive postures and activities, similar to those of China, Russia and the USA. As the situation unfolds in the context of the war in Ukraine and amidst escalating geopolitical tensions, the discourse surrounding offensive cyber operations is gaining in prominence. This includes concerns regarding attacks on critical and dual-use infrastructure and the growing involvement of non-state actors. The integration of emerging technologies such as AI into the cyber domain is expected to be a long-term and evolving trend.

To advance global cyber stability, the EU could consider exploring a direct or facilitative role in five respects: (*a*) deepening bilateral or multilateral exchange of acceptable and unacceptable cyber behaviour; (*b*) identifying off-

[78] Saalman, Su and Saveleva Dovgal, 'Cyber crossover and its escalatory risks for Europe' (note 2), p 20.

[79] Vorontsov (note 62); and Saalman, Su and Saveleva Dovgal, 'Cyber crossover and its escalatory risks for Europe' (note 2).

[80] Saalman, Su and Saveleva Dovgal, 'Cyber crossover and its escalatory risks for Europe' (note 2).

[81] Saalman, Su and Saveleva Dovgal, 'Cyber crossover and its escalatory risks for Europe' (note 2).

[82] European Commission, 'EU Policy on Cyber Defence' (note 1), pp. 1, 3 and 12. See also Väljataga, A., 'Cyber vigilantism in support of Ukraine: A legal analysis', NATO Cooperative Cyber Defence Centre of Excellence, Mar. 2022.

[83] Rodenhäuser T. and Vignati M., '8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them', International Committee of the Red Cross (ICRC) Humanitarian Law and Policy Blog, 4 Oct. 2023; and ICRC Global Advisory Board on Digital Threats during Armed Conflicts, *Protecting Civilians Against Digital Threats During Armed Conflict: Recommendations to States, Belligerents, Tech Companies, and Humanitarian Organizations* (ICRC: Geneva, 12 Oct. 2023.

limits critical infrastructure and articulating the escalatory risks associated with such attacks; (*c*) employing deconfliction lines and compartmentalizing cybersecurity amid intensified strategic competition; (*d*) expanding the discussion in cybersecurity by including a broader spectrum of participants and by exploring the multidomain cyber threats; (*e*) clarifying the role of the private sector and state obligations for restraining civilian participation in offensive cyber operations.

In particular, the EU should leverage its significant convening power to continue facilitating track-1 dialogues through its diplomatic channels with partner countries and, more importantly, with adversaries. Maintaining open channels of communication to foster understanding and cooperation in the realm of cyber diplomacy is vitally important in a turbulent global political environment. The EU should also work with major cyber stakeholders to achieve greater understanding on cyberattacks against dual-use infrastructure. This understanding can then be utilized to engage in knowledge-sharing and cooperative efforts to mitigate the risks associated with these cyberattacks.

Within the EU, documentation on member states' national debates over the development and application of offensive cyber capabilities, as well as their respective views on how to regulate the role of non-state actors in offensive cyber operations, are urgently needed. Developing a comprehensive view of each member state's domestic interests and policies will assist in policy formulation at the EU level. Discussions could be initiated by the Belgian presidency of the Council of the EU in January 2024, which could include suggestions for potential vehicles or platforms through which volunteers and hacktivists can be informed of the concerns over their involvement in offensive cyber activities. There is also a need to identify points of commonality and achieve consensus among EU member states on which critical infrastructure is off-limits for cyberattacks. This clarification can facilitate the development of a more unified stance at the EU level, while serving as an additional transparency measure in the EU's interactions with other international actors.

Finally, there is a role for research institutes to facilitate track-1.5 and track-2 dialogues focusing on engagement across domains (i.e. cyber, space and nuclear), with expanded participation by technical and industry experts. Diverse stakeholders can facilitate more granular exploration of trends in malware and cyber incidents to locate common challenges and potential solutions. Through EU and its member states' support, research institutes could conduct studies that compare experiences from other countries and from international organizations, such as the ICRC, regarding approaches to regulating the private sector and other non-state actors' involvement in cyber operations, particularly offensive ones. Their involvement can contribute to informing the debate and future legislation within the EU and to its serving as a model for promoting global cyber stability.

Abbreviations

AI	Artificial intelligence
CII	Critical information infrastructure
DARPA	Defense Advanced Research Projects Agency
DOD Cyber Strategy	US Cyber Strategy of the Department of Defense
EU	European Union
ICRC	International Committee of the Red Cross
ICT	Information and communication technology
IT	Information technology
NIS Directive	EU Network and Information Security Directive
PPP	Private–public partnership

RELATED SIPRI PUBLICATIONS

Mapping Cyber-related Missile and Satellite Incidents and Confidence-building Measures

Dr Lora Saalman, Larisa Saveleva Dovgal and Fei Su
SIPRI Insights on Peace and Security
November 2023

Cyber Crossover and Its Escalatory Risks for Europe

Dr Lora Saalman, Fei Su and Larisa Saveleva Dovgal
SIPRI Insights on Peace and Security
September 2023

The Role of Space Systems in Nuclear Deterrence

Nivedita Raju and Dr Tytti Erästö
SIPRI Background Paper
September 2023

Naval Incident Management in Europe, East Asia and South East Asia

Dr Ian Anthony, Fei Su and Dr Lora Saalman
SIPRI Insights on Peace and Security
March 2023

Cyber Posture Trends in China, Russia, the United States and the European Union

Dr Lora Saalman, Fei Su and Larisa Saveleva Dovgal
SIPRI Report
December 2022

Explaining the Nuclear Challenges Posed by Emerging and Disruptive Technology: A Primer for European Policymakers and Professionals

Andrew Futter
EUNPDC Paper
March 2021

Cyber-incident Management: Identifying and Dealing with the Risk of Escalation

Johan Turell, Fei Su and Dr Vincent Boulanin
SIPRI Policy Paper
September 2020

RECENT SIPRI PUBLICATIONS

Environmental Politics in Gulf Cooperation Council States: Strengthening the Role of Civil Society

Amal Bourhrous and Emelie Poignant Khafagi
SIPRI Research Policy Paper
November 2023

New Compact, Renewed Impetus: Enhancing the EU's Ability to Act Through its Civilian CSDP

Timo Smit
SIPRI Research Policy Paper
November 2023

The Arctic is Hot: Addressing the Social and Environmental Implications

Emilie Broek
SIPRI Policy Brief
September 2023

Integrating Gender Perspectives into International Humanitarian Law

Nivedita Raju and Laura Bruun
SIPRI Insights on Peace and Security
August 2023

Improving the Prospects for Peace in South Sudan: Spotlight on Measurement

Marie Riquier
SIPRI Policy Report
June 2023

Russia's Military Expenditure During Its War Against Ukraine

Professor Julian Cooper
SIPRI Insights on Peace and Security
June 2023

The Role of Umbrella States in the Global Nuclear Order

Dr Tytti Erästö
SIPRI Insights on Peace and Security
June 2023

Improving the Prospects for Peace in South Sudan: Spotlight on Stabilization

Dr Caroline Delgado
SIPRI Policy Report
May 2023

The World Food Programme's Contribution to Improving the Prospects for Peace in Sri Lanka

Dr Simone Bunse and Dr Vongai Murugani
SIPRI Policy Report
May 2023

SIPRI RESEARCH POLICY PAPER

ADVANCING THE ROLE OF THE EUROPEAN UNION IN PROMOTING GLOBAL CYBER STABILITY

FEI SU, LARISA SAVELEVA DOVGAL AND LORA SAALMAN

CONTENTS

ABOUT THE AUTHORS

Fei Su (China) is a Researcher with SIPRI's China and Asia Security Programme.

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

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