sipri

CYBER POSTURE TRENDS IN CHINA, RUSSIA, THE UNITED STATES AND THE EUROPEAN UNION

LORA SAALMAN, FEI SU AND
LARISA SAVELEVA DOVGAL

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

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

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

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

CYBER POSTURE TRENDS IN CHINA, RUSSIA, THE UNITED STATES AND THE EUROPEAN UNION

LORA SAALMAN, FEI SU AND
LARISA SAVELEVA DOVGAL

December 2022

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

Contents

Acknowledgements

The Stockholm International Peace Research Institute (SIPRI) and the authors would like to express their sincere gratitude to the German Federal Foreign Office for supporting this project with generous research funding and participation in its workshops. They would also like to thank the Observer Research Foundation America (ORF America) for providing support for the organization of an in-person workshop 'Cyber Postures and Dynamics: China, Russia, United States and Europe' hosted in Washington, DC under Chatham House Rule in November 2022.

The authors would like to express their appreciation for the valuable insights of the experts who engaged in interviews and who participated in the above-mentioned workshop. SIPRI and the authors would also like to recognize the institutions with which these over 35 experts are affiliated, including Amelsec, American Enterprise Institute, Carnegie Endowment for International Peace, Center for European Policy Analysis, Cyber Threat Alliance, Cyberspace Solarium Commission, European Council on Foreign Relations, Florida International University, Georgetown University, German Council on Foreign Relations, Harvard University, International Committee of the Red Cross, Microsoft, National Academies, National Defense University, ORF America, PIR Center, RAND Corporation, SINTEF Digital, Stanford University, Stiftung Neue Verantwortung, Stimson Center, Swedish Internet Foundation, Tsinghua University, Tufts University, University of Cincinnati, University of Maryland, Virginia University of Technology, United States Cyber Command and US Naval Academy.

Special thanks go to our external reviewers, as well as our SIPRI colleagues Dr Sibylle Bauer and Dr Vincent Boulanin for their constructive feedback on earlier drafts of the report. Finally, the authors also wish to express their sincere appreciation to SIPRI's Editorial Department for its significant contributions to realizing this final publication.

Abbreviations

AFSJ	Area of Freedom, Security and Justice
CDPF	Cyber Defence Policy Framework
CSDP	Common Security and Defence Policy
DHS	Department of Homeland Security
DOD	Department of Defense
EDA	European Defence Agency
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUMS	EU Military Staff
FBI	Federal Bureau of Investigation
FSARC	Financial Systemic Analysis and Resilience Center
FS-ISAC	Financial Services Information Sharing and Analysis Center
GDPR	General Data Protection Regulation
ICT	Information and communication technologies
IP	Internet protocol
ITU	International Telecommunications Union
JFT-CNO	Joint Task Force—Computer Network Operations
NATO	North Atlantic Treaty Alliance Organization
NIS Directive	Network and Information Security Directive
NSA	National Security Agency
OPM	Office of Personnel Management
PLA	People's Liberation Army
SCO	Shanghai Cooperation Organization
UN	United Nations
USCYBERCOM	US Cyber Command
5G	Fifth generation

Summary

Often applied at the organizational level, a cyber posture refers to a security architecture that facilitates prediction, prevention and mitigation of threats before, during and after a cyber intrusion and cyberattack. By contrast, this SIPRI Research Report examines cyber postures through the lens of key trends in China, Russia, the United States and the European Union (EU). The authors draw from primary sources in Chinese, English and Russian to identify unique concepts and terminology and to evaluate each of the actors' shifts in information security and cybersecurity, defensive and offensive operations, and deterrence and resilience. The findings challenge pre-existing assumptions that China and Russia are aligned on their information security and cybersecurity strategies. They also identify key points of difference between the EU and the USA in their regulatory structures in cyberspace, while highlighting areas in which the four actors increasingly intersect.

Chapter two reveals that China has been undergoing a shift in its cyber posture, with its defence white papers indicating that while 'information security' remains a primary concern, 'cybersecurity' is growing in prominence with concerns over both kinetic and non-kinetic operations. This suggests a development from a more reactive concept of 'active defence' to a more pre-emptive concept of 'proactive defence'. China promotes its holistic approach to cyberspace combining peacetime and wartime, and military and civilian organizations, which means that what may be perceived as a pre-emptive action by an adversary is what China considers a defensive continuous cycle of cyber operations to shape its internal and external environment. In terms of cyber governance, China has focused on multilateralization of international bodies to promote the technical foundations of its market share, cyber sovereignty and the Digital Silk Road.

Chapter three indicates that Russia maintains continuity in its cyber posture, with ongoing concerns over 'information security' and 'information warfare'. This translates into its lack of explicit reference to 'cybersecurity' in official documents, despite allegations of Russian kinetic cyber operations. Further, the division of information security and warfare into 'information-technological' and 'information-psychological' forms, means that the former term encompasses kinetic cyber operations, while the latter has begun to include an expansive concept of 'war against mentality'. Recognizing its inability to deny access and dependence on wider cyberspace networks, Russia has sought to leverage informational tools as 'deterrence by punishment'.

Chapter four describes how the USA's cyber posture has transitioned cyberspace from within its nuclear command structure to an independent domain. The US cyber strategy highlights the need to 'defend forward' and a holistic approach that highlights 'persistent engagement'. Recognizing the challenges of 'deterrence by denial' or 'zero defect', the USA has shifted to 'zero trust', which recognizes the inevitability of breaches and demands greater resilience and private sector engagement. This holistic approach also reflects growing concerns over US vulnerabilities to information operations, particularly through what has become labelled as disinformation.

Chapter five discusses the EU's unique position as a grouping of member states, which creates challenges to its realization of a unified cyber posture. As the EU's cyber regulations have expanded, the term 'cybersecurity' has attained prominence, yet reference to 'privacy and data protection' and 'network and information security' remains frequent. Recognizing that certain member states possess greater cybersecurity capacity, there is increasing need for and interest in fostering integrated EU cybersecurity legislation that will also facilitate its transition to becoming a global regulatory power in cyberspace. Despite the gradual buildup of its cyber resilience, the

EU remains conflicted on the employment of offensive cyber capabilities, preferring 'limited deterrence by punishment' via targeted sanctions against non-state actors.

Chapter six provides some conclusions on points of divergence and convergence among China, Russia, the USA and the EU. Among the divergences, China has started to integrate 'cybersecurity' into a narrative that mirrors that found in the USA, while Russia continues its adherence to an 'information security' focus within official and unofficial documents. In the case of the EU and the USA, they differ in their approaches towards offensive cyber operations, with the former more conflicted on their application at member state level. On convergences, both Russia and the USA have increasingly shifted from 'deterrence by denial' towards 'deterrence by punishment' in cyberspace through their forward-deployed strategies and offensive operations. Further, US efforts at greater integration between the public and private sector reflect aspects of China's 'military–civil fusion', which also seeks a more holistic approach to strengthen defensive and offensive capabilities. China, Russia and the USA all seek to balance defensive and offensive cyber operations through a continuous cycle of preparation, detection, mitigation, resilience and response through their concepts of 'proactive defence', 'active defence', 'defend forward' and 'persistent engagement'. While long denouncing Chinese and Russian controls on flows of information, the EU and the USA are also trending towards greater efforts to control, localize and leverage the transit of information. Thus, while there are points of divergence, China, Russia, the USA and the EU are all converging on cyberspace, potentially creating a platform for crisis management and negotiation. Nevertheless, these trends also suggest increasingly pre-emptive behaviour in cyberspace among three of the actors, requiring the EU to coordinate among its member states to re-evaluate and to better formulate its stance on offensive operations in its cyber posture.

1. Introduction

Examining the cyber postures of China, Russia, the United States and the European Union (EU) necessitates challenging pre-existing assumptions. It is often taken for granted that China and Russia are aligned in their concerns over the destabilizing role of information warfare in cyberspace. Yet Russian official discourse is singularly focused on information security, while China's official documents incorporate both information security and a parallel discourse on cybersecurity that mirrors US and EU narratives. Moreover, it is widely assumed that US and EU cyber postures are aligned, while differing starkly from those found in China and Russia. However, both the USA and the EU exhibit often contrasting regulatory structures in cyberspace, particularly when it comes to privacy and data localization. Further, their cyber postures increasingly reflect concerns found in China and Russia about the impact of information warfare on domestic stability.

At its most narrow application, a cyber posture refers to the overall strength of protocols for predicting, preventing and mitigating cyber threats, and the ability to act before, during and after an attack. It is predicated upon security policies, software, hardware, services, networks and information, managed through 'controls, policies or procedures'.[1] While such definitions are typically applied at the organizational level, this SIPRI Research Report seeks to examine key trends in how governments are shaping their cyber postures. The report posits that cyber posture is a dynamic concept, requiring understanding of strategic shifts along a spectrum that includes information security and cybersecurity, defensive and offensive operations, and deterrence and resilience.

Rather than providing a unified definition of each of these concepts, however, the report draws on primary sources to examine the unique terminology each of the four actors applies to the cyber domain.[2] The next four chapters identify key trends in the actors' evolving cyber postures, followed by a final chapter that identifies points of convergence and of divergence. These conclusions will serve as a foundation for a broader project that maps cyber posture trajectories along a spectrum and explores trilateral cyber dynamics among China, Russia and the USA to generate near-, medium- and long-term recommendations for the EU on navigating future escalation in cyberspace and enhancing global cyber stability.

[1] 'What is a cybersecurity posture and how can you evaluate it?', SecurityScorecard Blog, 19 Dec. 2019; and RiskXchange, 'What is a cyber security posture and how do you assess it?', [n.d.].

[2] Unless otherwise indicated, all translations from Chinese are by Dr Lora Saalman and from Russian by Larisa Saveleva Dovgal.

2. China's cyber posture

China has been undergoing a profound shift in its cyber posture. Its defence white papers indicate that while 'information security' (信息安全) remains a core concern, 'cybersecurity' (网络安全) is increasing in prominence, encompassing both kinetic and non-kinetic variants. This reflects a shift from a more reactive concept of 'active defence' (积极防御)—response to attack—to a more pre-emptive concept of 'proactive defence' (主动防御)—offensive anticipation of attack. Along with this transition, China's more holistic approach to cyberspace includes strategies that combine the phases of peacetime and wartime, as well as military and civilian organizations. Beyond domestic aims, China's standards are also shaping other countries' technological and regulatory structures through such concepts as 'cyber sovereignty' and such initiatives as the Digital Silk Road. The names and duties of the key Chinese organizations in the cyber domain are set out in table 2.1.

From information security to cybersecurity

Following its close observation of the USA's use of information superiority during the Gulf War in the early 1990s, China worked on leveraging its own information dominance to redress political, economic and military asymmetries.[3] By the end of the decade, two People's Liberation Army (PLA) colonels, Qiao Liang and Wang Xiangsui, developed a strategy—detailed in their book *Unrestricted Warfare*—for how China as a weaker country could defeat a technologically superior adversary.[4] Subsequently, the 2013 and 2020 editions of the PLA's publication *The Science of Military Strategy* reflected US writings on network-centric warfare and 'system-of-systems' (成体系系统) and an emphasis on asymmetric operations.[5] This points to a broader trend in which China has sought to both imitate and counter the USA as its primary adversary with advances in communications, satellite navigation and reconnaissance capabilities to enhance its own situational awareness, while developing the ability to affect the latter under an electronic 'fog of war'.[6]

Within this evolution, 'information security', with its focus on control over the flow of information and content, and on defending networks, has long been considered a broader concept than 'cybersecurity' in China.[7] More recently, however, Chinese official documents and the structure of military and civilian departments indicate that the concept of 'cybersecurity' is a growing part of both military and civilian spheres.[8] The establishment of China's Strategic Support Force and military white papers from 2015 and 2019 that focus on "cyber and information operations in warfare

[3] '海湾战争30周年启示之美军军改' [30th anniversary of the Gulf War and revelations of US military reform], *Xinhua Net*, 1 Apr. 2021.

[4] English translation: Qiao, L. and Wang, X., *Unrestricted Warfare: China's Master Plan to Destroy America* (Echo Point Books & Media: Brattleboro, VT, 2015).

[5] English translation: China Aerospace Studies Institute (CASI), *In Their Own Words: Science of Military Strategy 2020* (CASI: Montgomery, AL, Jan. 2022); and CASI, *In Their Own Words: Foreign Military Thought: Science of Military Strategy 2013* (CASI: Montgomery, AL, Jan. 2013).

[6] 黄成武、张剑 [Huang, C. and Zhang, J.] '拨开新的"战争迷雾"' [Clearing the new 'fog of war'], 解放军报 [*PLA Daily*] via 中华人民共和国国防部 [Chinese Ministry of Defence], 5 July 2022; and 军事科学院王保存少将 [Wang, C.], '直面军事变革—战争形态正在演变' [Confronting military change: The shape of war is evolving], 《瞭望》周刊 [*Outlook Weekly*], 16 July 2003 .

[7] Raud, M., 'China and cyber: Attitudes, strategies, organisation', NATO Cooperative Cyber Defence Centre of Excellence, 2016.

[8] 中华人民共和国国家互联网信息办公室 [Cyberspace Administration of China], '2022年上半年全国网络执法工作取得明显成效' [During the first half of 2022, national cyber law enforcement work has achieved remarkable results], 31 July 2022.

Table 2.1. Key Chinese cyber organizations and their roles and duties

Organization	Role and duties
Central Committee of the Communist Party of China (中国共产党中央委员会; CCCPC)	Responsible for the Network Security and Informatization Commission, which governs cultural and technical information security through the Cyberspace Administration of China
Central Cybersecurity and Informatization Commission (中央网络安全和信息化委员会; CCIC)	Formed under the CCCPC as Central Leading Group for Cybersecurity and Informatization; responsible for ensuring internet security, promoting digital economy and government interests, and internet censorship through the Public Opinion Information Center
Cyberspace Administration of China (国家互联网信息办公室; CAC)	Under the CCIC, supervises the National Computer Network and Information Security Management Centre; responsible for internet censorship systems; assumed control of the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC)
Ministry of Industry and Informatization Technology (工业和信息化部; MIIT)	Via the State Administration of Science, Technology, and Industry for National Defence, provides cyber agencies with talent from the Seven Sons of National Defence (Northwestern Polytechnical University, Harbin Engineering University, Harbin Institute of Technology, Beihang University, Beijing Institute of Technology, Nanjing University of Science and Technology, and Nanjing University of Aeronautics and Astronautics)
Ministry of Public Security (公安部; MPS)	Has network security protection detachments that secure domestic network infrastructure by identifying and investigating internet crimes, including harmful information
Ministry of State Security (国家安全部; MSS)	Responsible for cyber-enabled intelligence and counter-intelligence operations; supported by the 13th Bureau, known as the China Information Technology Evaluation Centre
Strategic Support Force (战略支援部队; SSF)	Overseen by the Central Military Commission (CMC) Joint Operations Command, via the CMC Joint Cyberspace Operations Command Centre; provides strategic information support and information operations; centralizes PLA warfare capabilities in space, cyberspace and electromagnetic domains

Note: Organizations are listed in English alphabetical order.

reflect China's integration of cyber, information, space and electromagnetic domains both operationally and strategically.[9] Further, the revised 'Cybersecurity review measures', approved at a meeting of the Cyberspace Administration of China in 2021, highlighted not only 'information security' but also a set of measures squarely focused on 'cybersecurity' threats.[10]

As part of this evolution, China's 2019 defence white paper exhibits a much more assertive and potentially offensive stance:

> Cyberspace is a key area of national security and economic and social development. Cybersecurity is a global challenge and a severe security threat facing China. The Chinese military has accelerated the construction of cyberspace forces, vigorously developed cybersecurity defence methods, and built a cyberspace defence force that is commensurate with China's international status and

[9] Costello, J. and McReynolds, J., 'China's Strategic Support Force: A force for a new era', Institute for National Strategic Studies, China Strategic Perspectives no. 13; 中华人民共和国国务院新闻办公室 [State Council of the People's Republic of China, Information Office], '新时代的中国国防' [China's national defence in a new era], 24 July 2019; and 中华人民共和国国务院新闻办公室 [State Council of the People's Republic of China, Information Office], '中国的军事战略' [China's military strategy], 26 May 2015.

[10] 中华人民共和国中央人民政府 [State Council of the People's Republic of China], '网络安全审查办法' [Cybersecurity review measures], 28 Dec. 2021.

compatible with that of a cyber power. China has strengthened the country's cyber border defences, detected and resisted cyber intrusions in a timely manner, and ensured the security of information networks to resolutely defend national cyber sovereignty, information security and social stability.[11]

Thus, while 'information security' remains a core concern, 'cybersecurity' as a term and concept has become an integral part of China's defence strategy. This includes a demarcated 'cyber border', indicating a domain that much like land, air, space or sea must be defended.

From active defence to proactive defence

While 'active defence' remains the bedrock of China's military doctrine, 'proactive defence' is an increasingly central element in its cyberspace strategy.[12] The PLA's concept of 'integrated network-electronic warfare' (网电一体战) dates to the early 2000s, when the former head of the Fourth Department of the PLA General Staff anticipated future information operations involving 'selecting key enemy targets and launching effective network-electronic attacks' through integrated cyber and electronic warfare.[13] Chinese official and non-official articles dating from 2018 through 2022 are also explicit about including proactive defence in China's evolution, including efforts to use pre-emption to thwart cyberattacks on its own critical infrastructure and to make its systems more resilient against attack and able to undertake offensive operations to intercept and destroy malware.[14]

This pre-emptive approach is holistic and typified by a wider strategy of 'peacetime–wartime integration' (平战结合、平战一体), which maintains that cyber operations require a domain-centric force structure predicated on continuous 'integrated reconnaissance, attack, and defence' (侦攻防一体化).[15] This structure has contributed to allegations that China engages in dispersed cyber espionage campaigns—from universities to industries to militaries—to continuously shape its strategic environment and to access both the information 'high ground' and dual-use or military-grade equipment and advanced technologies.[16] This strategy's lack of distinction between a time of war and a time of peace, similar to the crossover in China's broader 'military–civil fusion' (军民融合) strategy, also means that what China views as defensive may be viewed by an adversary as pre-emptive.[17] In other words, if China is engaged in a continuous set of operations to thwart cyber intrusions and attacks, it is always in defence mode instead of attack mode.

[11] 中华人民共和国国务院新闻办公室 [State Council of the People's Republic of China, Information Office], '新时代的中国国防' [China's national defence in a new era] (note 9).

[12] Saalman, L., *Multidomain Deterrence and Strategic Stability in China*, SIPRI Insights on Peace and Security no. 2022/2, Jan. 2022.

[13] Costello and McReynolds (note 9).

[14] 中华人民共和国国家互联网信息办公室 [Cyberspace Administration of China], '我国首部关键信息基础设施安全保护国家标准在京发布' [First national standard for critical information infrastructure security protection released in Beijing], 9 Nov. 2022; 中华人民共和国国家互联网信息办公室 [Cyberspace Administration of China], '国家网络安全宣传周专家观点：保障赛博空间安全就是保障国家主权' [National cybersecurity publicity week expert opinion: Ensuring cyberspace security is ensuring national sovereignty], 14 Oct. 2021; 国家保密局 [National Administration of State Secrets Protection], '网络空间动态防御技术' [Cyberspace dynamic defence technology], 11 Dec. 2020; and 驭龙 [Yu, L.], '走出隐藏边界，实施主动防御' [Stepping out of hidden boundaries, implementing proactive defence]', *SEC-UN* 安全村 [*Security Village*], 26 Mar. 2018.

[15] Costello and McReynolds (note 9).

[16] US Department of Defense (DOD), *Military and Security Developments Involving the People's Republic of China 2022*, Annual Report to Congress, 29 Nov. 2022, pp. xii–xiii; and Krekel, B., Adams, P. and Bakos, G., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Northrop Grumman report prepared for the US–China Economic and Security Review Commission, 7 Mar. 2012.

[17] 中华人民共和国外交部 [Chinese Ministry of Foreign Affairs], '军民融合' [Military–civil fusion], 1 Apr. 2021; and 国务院关于印发 [Chinese State Council on Printing and Distributing], 新一代人工智能发展规划的通知 [Notice of the new generation of artificial intelligence development plan], 国发 35 [National Law no. 35], 8 July 2017.

From cyber vulnerability to cyber sovereignty

Concerns over 'colour revolutions' (颜色革命) or anti-regime protest movements have been central in shaping China's concept of 'information security', and even 'cybersecurity'.[18] As China pursues enhanced digitization and a role as a 'cyber power' (网络强国), recognition of its dependence on cyberspace as both a vulnerability and a strength has grown.[19] To this end, China has strengthened what has become known as the Great Firewall, with keyword filters and targeting of virtual private networks.[20] Yet, while this mitigates concerns over information flows weakening China's internal stability, China still faces challenges to its network security. Given its reliance on externally provided software and hardware, China has launched indigenization efforts to alleviate vulnerabilities in its domestic system and foreign supply chain, through such initiatives as strengthening encryption with quantum computing and manufacturing its own chips and semiconductors.[21] The impetus came from such seminal events as Microsoft ending its support of Windows XP systems, which were pervasive in China, and the Edward Snowden revelations about the scope of US cyber espionage.[22]

Chinese concerns over external reliance also include normative and governance structures, stemming from US dominance of everything from root servers to agreements.[23] China has focused on multilateralization, through calls for an international internet treaty and formation of an intergovernmental internet organization, as well as reasserting the importance of the United Nations in its 2010 internet white paper.[24] China has also emphasized 'cyber sovereignty'—in which use of cyberspace within a state's territory, by both domestic and foreign citizens, is to be controlled by the host state. Accordingly, China and several Shanghai Cooperation Organisation (SCO) members submitted to the UN General Assembly a draft in 2011, and a revised version in 2015, of the International Code of Conduct for Information Security, which embedded information security and cybersecurity into the 'sovereignty, territorial integrity and political independence of all states'.[25] China has also expanded its involvement in the UN group of government experts on Developments in the Field of Information and Telecommunications in the Context of International Security, contributing to a consensus document in 2013 which stated that 'international law, and in particular, the UN Charter, applies to cyberspace', such "that 'State sovereignty and international

[18] 释启鹏、韩冬临 [Shi, Q. and Han, D.], '当代社会运动中的政权崩溃—"颜色革命"与"阿拉伯之春"的定性比较分析' [Regime collapse in contemporary social movements: A qualitative comparative analysis of 'colour revolutions' and 'Arab Spring'], 国际政治科学 [*Quarterly Journal of International Politics*], vol. 2, no. 1 (2017); and 王越 [Wang, Y.], '"颜色革命"是如何摧毁乌克兰的' [How the 'colour revolution' destroyed Ukraine], 这就是中国 [*This is China*], no. 149 (4 July 2022).

[19] 中国信息通信研究院 [China Academy of Information and Communications Technology], '中国网络安全产业白皮书' [China's Cybersecurity Industry White Paper], no. 202201, Jan. 2022.

[20] Creemers, R., 'China's cyber governance institutions', Leiden Asia Center, Jan. 2021.

[21] '微软强制XP系统退休,中国忧该计划与监视有关' [Microsoft forces XP system to retire, China worries about surveillance-related plan], 参考消息网 [Reference News Network], 11 Mar. 2011; and 中华人民共和国国务院 [State Council of the People's Republic of China], '国务院关于印发《中国制造2025》的通知' [Notice of the State Council on issuing 'Made in China 2025'], 国发 28 [National Law no. 28], 8 May 2015.

[22] 鲁传颖 [Lu, C.], '"斯诺登事件"与网络空间安全困境' [The 'Snowden incident' and the cyberspace security dilemma], 安全内参 [*Security Internal Reference*], 19 Dec. 2018; and '微软强制XP系统退休,中国忧该计划与监视有关' [Microsoft forces XP system to retire, China worries about surveillance-related plan] (note 21).

[23] Internet Corporation for Assigned Names and Numbers (ICANN), 'Contract between ICANN and the United States government for performance of the IANA function', 9 Feb. 2000.

[24] Xinhua, 'Full text: White paper on the internet in China', via *China Daily*, 8 June 2010.

[25] United Nations, General Assembly, 'Letter dated 9 January 2015 from the permanent representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General', A/69/723, 13 Jan. 2015; and Chinese Ministry of Foreign Affairs, 'International Code of Conduct for Information Security', 12 Sep. 2011.

norms and principles that flow from sovereignty apply to State conduct'.[26] Reference to the UN Charter and state sovereignty fits into China's concept of 'cyber sovereignty' as articulated in its 2016 National Cyber Strategy. It further illustrates China's ongoing concerns over maintaining social order and limiting external interference in its internal affairs via cyberspace.

From national standards to global standards

In promoting cyber sovereignty and its national model, China has sought to shape global information, technology and cyber standards. After joining the World Trade Organization in 2001, China mounted an effort to define standards in software, hardware and communication technologies with the view that controlling a standard ensured the capture of market value. Chinese officials have come to lead such organizations as the International Organization of Standardization, the International Electrotechnical Commission and the International Telecommunications Union (ITU). Chinese leadership of the ITU led to its 2020 proposal of a new internet protocol (IP) to replace the current foundation of the global internet, in greater alignment with its own national measures to utilize IP version 6. China has also been active in trying to define standards for wireless local-area network authentication and privacy infrastructure, audio-video coding and radio frequency identification.

Further, in 2015 China sent more than 40 delegates to a meeting of the Internet Engineering Task Force, while delegates from Huawei numbered twice that of other telecommunications companies at a 2016 meeting in Vienna to define specifications of fifth-generation (5G) mobile networks—moves that some have labelled 'swarming of the global governance agenda'.[27] More broadly, China's Digital Silk Road has created a conduit via which Chinese systems serve as the backbone of telecommunications, artificial intelligence capabilities, cloud computing, e-commerce and mobile payments, surveillance technology and smart cities in Belt and Road Initiative countries.[28] Rather than simply garnering market share, these moves indicate a broader agenda to shape norms and the future of cyberspace.

[26] United Nations, General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/68/98, 24 June 2013; and Charter of the United Nations, Article 2.

[27] Segal, A., 'Chinese cyber diplomacy in a new era of uncertainty', Hoover Institution Aegis Paper no. 1703, 2 June 2017.

[28] 中华人民共和国商务部 [Chinese Ministry of Commerce], '后疫情时代，数字丝绸之路价值将更为彰显' [In the post-pandemic era, the value of the digital silk road will be more prominent], 16 Aug. 2020.

3. Russia's cyber posture

Russia maintains a strong continuity in its cyber posture, characterized by its ongoing concerns over 'information security' (информационная безопасность) and 'information warfare' (информационное противоборство). Official and even non-official documentation tends to lack explicit reference to 'cybersecurity' (кибербезопасность), despite allegations of Russian kinetic operations in cyberspace. Nevertheless, cybersecurity is not entirely missing from this discourse, as Russia's information security strategies also contain a technical or kinetic form, alongside the more commonly discussed psychological form labelled by some as 'disinformation'. In more recent years, this has shifted to a more expansive concept of 'mental war' or 'war against mentality' (ментальная война) that seeks to shape civic and cultural foundations. Recognizing its own vulnerabilities, through its inability to deny access and dependence on wider cyberspace networks, Russia has sought to leverage informational tools as 'deterrence by punishment'. The names and duties of the key Russian organizations in the cyber domain are set out in table 3.1.

From information security to cyber sovereignty

Russia has introduced several indigenous elements to its cyber strategy both in terms of concepts and application.[29] Russian national strategic concepts, doctrines and laws refer to 'information security' and 'information warfare', rather than to 'cyber' security or warfare.[30] Information security and warfare are both further subdivided conceptually into 'information-technological' (информационно-технологический) and 'information-psychological' (информационно-психологический) forms. An earlier definition of 'information warfare', dating back to the mid 1990s, suggests that it encompassed both psychological effects and 'operating in less of a fog of war than the adversary'.[31] These definitions continue to be reflected in Russia's conception of cyberspace and its ability to affect it through information and communication technologies (ICT), including computer hardware, cyber and information security threats, and information-psychological warfare that also features taking control of the adversary's narrative to influence its behaviour.[32]

Russia's current approach to information security emerged at the beginning of the 2000s, following the release of the first Russian information security doctrine in the post-Soviet era. In this, Russia identified key threats to its information security in the 'desire of a number of countries to dominate and infringe on Russia's interests in the global information space, to oust it from the external and internal information markets'.[33] The approach was largely reactive, lacking a systematic assessment of the kind of threats large foreign ICT companies could pose to Russian interests. As Russia's inability to control the global network became apparent, its leaders focused on formulating a vision of information sovereignty, essentially confined by its territorial

[29] Zabierek, L. et al., *US–Russian Contention in Cyberspace: Are "Rules of the Road" Necessary or Possible?* (Belfer Center for Science and International Affairs: Cambridge, MA, June 2021), pp. 37–38.

[30] Connell, M. and Vogler, S., 'Russia's approach to cyber warfare', CNA Occasional Paper, Mar. 2017.

[31] Thomas, L. T., 'Russian view on information-based warfare', *Airpower Journal*, special edn, 1996, p. 27.

[32] Tashev, B., Purcell, M. and McLaughlin, B., 'Russia's information warfare: Exploring the cognitive dimension', *Marine Corps University Journal*, vol. 10, no. 2 (2019), pp. 130–31.

[33] 'Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895)' [Doctrine of Information Security of the Russian Federation, approved by the President on 9 September 2000], Российская газета [*Russian Newspaper*], 15 Sep. 2000.

Table 3.1. Key Russian cyber organizations and their roles and duties

Organization	Role and duties
Federal Security Service (Федеральная служба безопасности; FSB)	Responsible for equipment surveillance; intercepting, decrypting and processing of electronic messages; and technical penetration of foreign targets; created the National Coordination Center for Computer Incidents (RU-CERT)
Federal Service for Supervision of Communications, Information Technology and Mass Media (Роскомнадзор; Roskomnadzor or RKN)	Subordinate to the Ministry of Digital Development; controls and supervises mass electronic media, communications, telecommunications, information technology, personal data, and radio frequency systems
Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Главное управление Генерального штаба Вооружённых сил РФ; GRU)	Subordinate to the Ministry of Defence; collects, analyses and summarizes information about the military-political situation with regard to Russian security interests; alleged to possess special units for cyber operations targeting civil and military infrastructure
Ministry of Defence (Министерство обороны; MOD)	Created the Information Operations Force, which is tasked with protecting military control and communication systems from cyberterrorism and making military-sensitive information inaccessible to adversaries
Ministry of Digital Development, Communications and Mass Media (Министерство цифрового развития, связи и масссовых коммуникаций; MDDCMM)	Previously called the Ministry of Communications of the former Soviet Union; develops and implements state policies on information and communications technologies, digital media and personal data processing
Ministry of Foreign Affairs (Министерство иностранных дел; MFA)	Created the Department of International Information Security, which is tasked with implementing state policies on international information security
Security Council of the Russian Federation (Совет безопасности Российской Федерации; SCRF or Sovbez)	Formed an interdepartmental commission to ensure national technological sovereignty of critical information infrastructure

Note: Organizations are listed in English alphabetical order.

borders.[34] Sovereignty and territorial integrity of Russia's cyberspace domain are named as key information security priorities in the 2016 Information Security Doctrine.[35] This has expanded into Russia's support, alongside that of China and other SCO members, in international forums of 'cyber sovereignty'.[36]

By the late 2000s, Russia's focus started to shift towards the synergy of 'military' (военный) and 'non-military' (невоенный) forms of warfare. Ambitions to achieve military preponderance over Russia 'primarily in strategic nuclear forces, through the development of high-precision, information and other high-tech means of warfare', espoused by its adversaries, were deemed highly detrimental to Russian military security.[37] Russia responded to these threats with its own long-term vision of national secur-

[34] Vendil Pallin, C. and Hjelm, M. 'Moscow's digital offensive: Building sovereignty in cyberspace', Swedish Defence Research Agency, FOI Memo, Apr. 2021.

[35] Доктрина информационной безопасности Российской Федерации [*Doctrine of Information Security of the Russian Federation*], Официальные сетевые ресурсы Президента России [Official internet resources of the President of Russia], 5 Dec. 2016.

[36] United Nations, General Assembly, A/69/723 (note 25); and Chinese Ministry of Foreign Affairs, 'International Code of Conduct for Information Security' (note 25).

[37] 'Стратегия национальной безопасности Российской Федерации до 2020 года' [National Security Strategy of the Russian Federation until 2020], Официальные сетевые ресурсы Президента России [Official internet resources of the President of Russia], 13 May 2009; and 'Стратегия национальной безопасности Российской

ity and ICT within its long-sought priority of information sovereignty.[38] It required ICT companies operating in Russia to store personal data locally; to shift to using domestic software and hardware; and to build capabilities for protecting critical information infrastructure that would deflect and enable recovery from hostile activities in cyberspace. Further, cyberspace operations became a means to 'level the playing field' in view of political, economic and military asymmetries vis-à-vis its adversaries.[39] This subsequently led to the proliferation of cybercrime groups pledging support for the Russian government while allegedly engaging in dispersed operations targeting all levels of both domestic and foreign society.[40]

From information-psychological warfare to war against mentality

Russian threat perceptions coupled with a deteriorating international environment have significantly impacted domestic conceptions of information-psychological warfare. In earlier versions of Russian strategic documents, information-psychological security threats were described as 'threats to the constitutional rights and freedoms of man and citizen in the field of spiritual life and information activities, individual, group and public consciousness', materializing through the 'illegal use of special means of influencing individual, group and public consciousness'.[41] The perceived and real hostility of the West towards Russia also emerged in the latter's concerns about cultural sovereignty, resulting in a proclamation of the 'application of information technologies in the interests of preserving the cultural, historical, spiritual and moral values of the multinational people of the Russian Federation' as a national interest to be safeguarded by information security.[42] Thus, a key goal of Russia has been to 'neutralize' the impact on its information infrastructure and its people, individually and as a group, which could undermine 'the historical foundations and patriotic traditions associated with the defence [of Russia]'.[43]

Following the 2014 Crimean crisis and the intensification of information campaigns both targeting and emanating from within Russia, the concept of national interest shifted from safeguarding individual and group consciousness to the 'development of a safe information space, [and] protection of Russian society from destructive information and psychological impact', found in both the 2015 and 2021 versions of Russia's National Security Strategy.[44] Thus, the survival of the state became intertwined with the ability of individuals and society to withstand the broader spectrum of threats conceived of as 'war against mentality'.[45] As such, 'psychological warfare' refers to

Федерации' [National Security Strategy of the Russian Federation], Официальные сетевые ресурсы Президента России [Official internet resources of the President of Russia], 31 Dec. 2015.

[38] Карасёв, П. и Стефанович, Д. [Karasev, P. and Stefanovich, D.], 'Кибербезопасность критически важной инфраструктуры: новые вызовы' [Cybersecurity of critical infrastructure: New challenges], Россия в глобальной политике [*Russia in Global Affairs*], vol. 20, no. 6 (2022).

[39] Views of experts expressed at the workshop 'Cyber postures and dynamics: China, Russia, United States and Europe', SIPRI and the Observer Research Foundation America, Washington, DC, 2–3 Nov. 2022.

[40] Interviews with two US cyber experts in Washington, DC, 4 Nov. 2022; and Cybersecurity and Infrastructure Security Agency, 'Russian state-sponsored and criminal cyber threats to critical infrastructure', Alert no. AA22-110A, 20 Apr. 2022.

[41] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895) [Doctrine of Information Security of the Russian Federation] (note 33).

[42] Доктрина информационной безопасности Российской Федерации [Doctrine of Information Security of the Russian Federation] (note 33).

[43] Доктрина информационной безопасности Российской Федерации [Doctrine of Information Security of the Russian Federation], (note 33).

[44] 'Стратегия национальной безопасности Российской Федерации' [National Security Strategy of the Russian Federation], Официальные сетевые ресурсы Президента России [Official internet resources of the President of Russia], 2 July 2021.

[45] Коровин, В. [Korovin, V.], 'Что такое ментальная война' [What is mental war?], Взгляд [*View*], 29 Mar. 2021.

direct information operations by an adversary in the context of a situation or conflict, sometimes called disinformation campaigns. War against mentality aims at changing the 'consciousness, worldview, goals, values and priorities of a society', that is, the foundations of its civilization.[46] Further, this has impacted how information warfare has been increasingly perceived by Russian leadership. Rather than distinguishing between peacetime and wartime, the Russian concept of warfare against mentality has become a holistic one, to be applied at all times and to all parts of society. That is, embracing the use of non-military means to achieve political goals by engaging the adversary below the threshold of armed conflict, the concept of 'war against mentality' provides for being in a 'permanent and protracted conflict'.[47]

Not only has Russia's perception of information warfare changed, but so has its vision of what that warfare effectively does. Russian political–military thought has begun to explore and exploit the concept of 'reflexive control' (рефлексивное управление) of an adversary, which entails manipulating the latter's behaviour by 'implementing measures and actions that incite the enemy to act in a corresponding way that is advantageous for [Russia]'.[48] Portrayed as a defensive response against Western information dominance, reflexive control connotes what Russia perceives as legitimate efforts to project national power and a favourable national discourse through information campaigns to change public worldviews in other countries—particularly in the post-Soviet space—by making them 'question anything and everything coming from the West'.[49]

While 'information-psychological', 'warfare against mentality' and 'reflexive control' operations continue to dominate, however, they remain paired with 'information-technical' operations.[50] This suggests that in addition to combating and leveraging hybrid means of warfare to inflict psychological impacts, Russian entities are also empowered to conduct cyber warfare through technical or kinetic means. In recognition of this, in March 2022, a group of human rights lawyers sent a formal request to the Office of the Prosecutor for the International Criminal Court in the Hague, urging war crime prosecutions of both official and unofficial Russian hackers for alleged kinetic cyberattacks against Ukraine's electricity facilities in 2015 and its capital in 2016.[51]

From deterrence by denial to deterrence by punishment

The reliance of Russian political and military leadership on countering information-security threats, building credible protection systems and ensuring information sovereignty suggests that Russia has long viewed its information and cyber capabilities through a strategy of 'deterrence by denial' (сдерживание посредством недопущения). Largely following the logic of deterrence in the nuclear domain, this entails denying potential adversaries the ability to threaten Russian security using information-technological means. However, following allegations of Russian interference in the 2016 US presidential election, official rhetoric in Russia started to show signs of 'deterrence by punishment' (сдерживание посредством наказания)—threatening to

[46] Ильницкий, А. [Ilnitskiy, A.], 'Ментальная война России' [Russian mental war], Военная мысль [*Military Thought*], 16 Aug. 2021.

[47] Cunningham, C., 'A Russian Federation information warfare primer', Henry M. Jackson School of International Studies, University of Washington, 12 Nov. 2020.

[48] Чаусов, Ф. [Chausov, F.], 'Управление боем на основе рефлексивного анализа обстановки' [Command and control of battle on the basis of a reflexive analysis of the situation], *Morskoi Sbornik* [*Navy Journal*], no. 6 (2017).

[49] Kofman, M. and Rojansky, M., 'A closer look at Russia's "hybrid war"', Kennan Cable, no. 7, Apr. 2015.

[50] Interview with Russian cyber expert, Washington, DC, 4 Nov. 2022; Kofman, M. et al., 'Russian military strategy: Core tenets and operational concepts', Center for Naval Analyses, Aug. 2021; and Medvedev, S. A., 'Offense–defense theory analysis of Russian cyber capability', Naval Postgraduate School, Mar. 2015.

[51] Greenberg, A., 'The case for war crimes charges against Russia's Sandworm hackers', *Wired*, 12 May 2022.

inflict damage that nullifies an adversary's potential gains from a cyberattack. Referring to US threats to 'retaliate for the Russia cyberattacks', Russia's special representative for international information security stated that 'force breeds counterforce . . . live by the (cyber) sword, die by the sword'.[52]

Nevertheless, the change in rhetoric seemingly did not lead to an explicit policy change, as Russia's 2020 Military Doctrine continued to emphasize that to deter and prevent military conflict, Russia must create such conditions that 'reduce the use of ICT for military-political purposes'.[53] Instead, the resultant deterrence strategy is a balance between denial and punishment, predicated on development of forces and methods of 'information confrontation' (информационное противоборство).[54] Yet this balance does not specify the nature of these methods nor their intent. The flexibility of Russia's approach to information warfare has enabled it to tailor its information and cyber efforts to its broader understanding of its own political–military aims. Earlier versions of Russia's strategic documents indicate the prevalence of non-military measures over military measures in modern conflicts, with an emphasis on 'early implementation of information warfare measures to achieve political goals without the use of military force, and subsequently—in the interest of forming a favourable reaction of the world community to the use of military force', while later versions shifted to integrated non-military and military means.[55]

Empirically, this shift is evident in alleged Russian activities from the mid-2000s that applied cyber 'pressure to affect outcomes' in Estonia, to those of the mid-2010s that used cyber and information warfare alongside military conflicts in Georgia and conducted simultaneous information, cyber and military campaigns in Ukraine.[56] Whether state or non-state, these activities suggest an effort both to expand such activities in cyberspace and to enhance other military and political capabilities.[57] Conceptually, this approach tends to be labelled as 'active defence'. In the Russian case, this term may be defined as the employment of pre-emptive, non-military measures to disrupt an adversary's systems and networks, followed by imposition of information superiority once there is full-scale military engagement.[58] As noted by some experts from Russia, however, the essence of information warfare 'lies in the dominant control with the help of computer technology and means of communication of the information space'.[59] The shift from a 'focus on cyber-attacks on infrastructure . . . towards information operations' reflects Russia's evolution towards a more assertive cyber posture.[60]

[52] Шакиров, О. [Shakirov, O.]., 'Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве' [Whoever comes with a cyber sword: The approaches of Russia and the United States to deterrence in cyberspace], Международная аналитика [*International Analytics*], vol. 11, no. 4 (2020).

[53] 'Военная доктрина Российской Федерации' [Military Doctrine of the Russian Federation], МЧС России [Russian Ministry for Civil Defence, Emergencies and Elimination of Consequences of Natural Disasters], 25 Dec. 2014.

[54] 'Военная доктрина Российской Федерации' [Military Doctrine of the Russian Federation], МЧС России 25 Dec. 2014 (note 53).

[55] 'Военная доктрина Российской Федерации' [Military Doctrine of the Russian Federation], Официальные сетевые ресурсы Президента России [Official Internet Resources of the President of Russia], 5 Feb. 2010.

[56] Lloyd, G., 'Hybrid warfare and active measures', *Small Wars Journal*, 10 Oct. 2021; and Jaitner, M., 'Russian information warfare of 2014', 7th International Conference on Cyber Conflict: Architectures in Cyberspace, 2015.

[57] Bokśa, M., 'Russian information warfare in Central and Eastern Europe: Strategies, impact, countermeasures', German Marshall Fund of the US (GMF) Policy Paper no. 15, June 2019; and Kristiansen, M. and Hoem, N., 'Russian cyber strategy', *Small Wars Journal*, 14 Feb. 2021.

[58] Thomas, T., 'Russian military thought: Concepts and elements', MITRE, Aug. 2019; and Tirpak, J., 'Strategy & policy: The Russian way of war', *Air & Space Forces Magazine*, 7 Oct. 2021.

[59] Рубанов, В. [Rubanov, V.], 'Информационная война и цифровой мир' [Information war and digital peace], Независимая газета [*Independent Newspaper*], 26 Apr. 2016.

[60] Rugge, F. (ed.), *Confronting an 'Axis of Cyber'? China, Iran, North Korea, Russia in Cyberspace* (Ledizioni LediPublishing: Milan, 2018).

4. The United States' cyber posture

The USA's cyber posture has changed from embedding cyberspace within its nuclear command structure towards treating it as an independent domain. This evolution has occurred in tandem with US attempts to balance the pervasive impact of cyberspace on all levels of society. Recognizing the challenges of a strategy that aims to ensure 'deterrence by denial' or 'zero defect', the USA has shifted to an approach of 'zero trust', which acknowledges that breaches are inevitable and must be met with cyber resilience, requiring multi-stakeholder engagement. The USA has factored both military and civilian organizations into this structure and made efforts to engage the private sector. This holistic approach also reflects an increasing concern over the use by adversaries of information—or disinformation—to exploit US transparency and dependence on cyberspace. The names and duties of the key US organizations in the cyber domain are set out in table 4.1.

From information space to cyber domain

As early as 1972 the USA recognized the need for comprehensive computer security and defence, expanding these efforts in the following decades to reduce vulnerabilities and to protect information systems in the face of hacking incidents, cyber espionage and equipment malfunctions.[61] By 1997, the offensive side of such cyber operations came to the fore when the US secretary of defense 'officially delegated authority' to the National Security Agency (NSA) to develop computer network attack 'operations to disrupt, deny, degrade or destroy' information in target computers or networks, 'or the computers and networks themselves', with exercises like Eligible Receiver 97 pitting NSA programmers against US military defenders.[62] This prompted the US military to establish the Joint Task Force—Computer Network Defense, which became the Joint Task Force—Computer Network Operations (JFT-CNO) in 1999.[63] Around this time, in 1998, RAND released a report on the intersection of software and hardware vulnerabilities, indicating the bridging of information warfare and cyber warfare into something more kinetic, as with potential cyberattacks on energy, telecommunications or other grids and providers.[64]

Building on this transition from information to kinetic concerns, the 2004 National Military Strategy of the USA, prepared by the US Joint Chiefs of Staff, declared cyberspace one of the 'domains of the battlespace' alongside air, land, sea and space.[65] That same year, the JTF-CNO was divided into defensive and offensive components, respectively the Joint Task Force—Global Network Operations and the Joint Functional Component Command—Network Warfare, operating under the US Strategic Command. In 2009 the two task forces were merged again to create a new command, US Cyber Command (USCYBERCOM), with an articulated domain of operations 'to integrate, synchronize and conduct the full spectrum of cyberspace operations'.[66] The result was the much-debated dual-hat arrangement under which both the NSA and

[61] US Cyber Command, 'Our history', [n.d.].

[62] Black, W. B., 'Thinking out loud about cyberspace', *Cryptolog* (Spring 1997), via National Security Archive, Doc. ID 4033695; and National Security Archive, 'Eligible receiver 97: Seminal DOD cyber exercise included mock terror strikes and hostage simulations', 1 Aug. 2018.

[63] National Security Archive, 'Joint Task Force—Computer Network Defense: 20 years later', 19 June 2019.

[64] Ware, W. H., *The Cyber-Posture of the National Information Infrastructure* (RAND Corporation: Santa Monica, CA, 1998).

[65] US Joint Chiefs of Staff (JCS), *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow* (Office of the JCS: Washington, DC, 2004), p. 18.

[66] US Cyber Command, 'Our history' (note 61).

Table 4.1. Key United States cyber organizations and their roles and duties

Organization	Role and duties
Cyber Command (USCYBERCOM)	Combatant command within the Department of Defense (DOD); responsible for defending information systems, supporting joint force commanders with cyberspace operations and defending country from significant cyberattacks; engages in defensive and offensive cyber operations; service cyber partners include Army Cyber Command, Fleet Cyber Command/Tenth Fleet, Sixteenth Air Force/Air Forces Cyber, Marine Corps Forces Cyberspace Command, Cyber National Mission Force and Joint Force Headquarters—DOD Information Network
Cybersecurity and Infrastructure Security Agency (CISA)	Serves as cyber defence agency and coordinator for critical infrastructure security and resilience; engages public and private sectors through the Joint Cyber Defense Collaborative
Department of Homeland Security (DHS)	Through its Science and Technology Directorate, Homeland Security Advanced Research Projects Agency and Cyber Security Division, supports research, development, testing, evaluation and transition of cybersecurity and information assurance technologies; Cyber Security Division created the US Computer Emergency Readiness Team (US-CERT)
Department of State (DOS)	Established the Bureau of Cyberspace and Digital Policy to lead work on cyberspace and digital diplomacy; addresses national security challenges, economic opportunities and values across cyberspace, digital technologies and digital policy
Federal Bureau of Investigation (FBI)	Its rapid-response Cyber Action Team investigates cyberattacks and intrusions; collects and shares intelligence; receives reports from the public via its Internet Crime Complaint Center; tracks incidents through its CyWatch operations centre
National Security Agency (NSA)	Provides foreign signals intelligence and intelligence on cyber threats and information; develops nuclear command and control threat, vulnerability, risk and cryptographic services; releases integrated threat, assessment, mitigation and protection products; executes cryptography and security engineering; engages in combined defence/offence operations and information sharing via Cybersecurity Directorate and Cybersecurity Collaboration Center

Note: Organizations are listed in English alphabetical order.

USCYBERCOM have the same leader, which has led to questions as to whether their difference in nature—with the former responsible for 'quiet' signals intelligence and the latter responsible for 'loud' offensive operations—hinders their respective missions.[67]

From deterrence by denial to deterrence by punishment

There has long been a US concern about the inability to deter in cyberspace, particularly through deterrence by denial.[68] In recognition of inherent system vulnerabilities, there has been an increasing shift towards a form of deterrence based on 'cost imposition', in which the potential consequences of an action are intended to thwart

[67] Pomerleau, M., 'Key lawmakers in favor of keeping "dual hat" arrangement between Cybercom and NSA', *DefenseScoop*, 17 Nov. 2022.

[68] Jaikaran, C., 'Cybersecurity: Deterrence policy', Congressional Research Service Report no. R47011, 18 Jan. 2022; Pomerleau, M., 'Cyber Command nominee: Attacks must come with a cost', *C4ISR*, 1 Mar. 2018; and Paul, C., Porche, I. R. and Axelband, E., *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces* (RAND Corporation: Santa Monica, CA, 2014).

an adversary.[69] While this concept, alongside 'deterrence by resilience', continues to gain traction, it has been difficult to execute in practice.[70] As noted by the former heads of the US Army's Cyber Directorate and USCYBERCOM, in contrast to the relatively straightforward permissions required for kinetic operations, a cyber operation against, for example, a power plant could 'only be used if an execute order authorized cyber operations, that particular power plant was already on a cyber targeting list, the cyber operators already performed appropriate operational preparation of the environment on the power plant's network, and interagency and possibly international deconfliction had taken place'.[71] This has led some to argue for an end of the USCYBERCOM and NSA dual-hat leadership, which is seen as complicating the former's approval process and contributing to its risk aversion.[72] Nevertheless, others emphasize that this structure should remain, since it facilitates interagency team coordination and enhances capacity, while imposing legal obligations under the Law of Armed Conflict.[73]

The US Department of Defense (DOD) cyber strategy of 2018 and its first cyber posture review of the same year are essential to understanding this evolving risk calculus in cyberspace.[74] The US cyber strategy highlights the need to 'defend forward', that is, to 'disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict', described by some as 'continuous pre-emption'.[75] The strategy also highlights the need for 'persistent engagement', that is, '[p]roactively engaging in the day-to-day great power competition in cyberspace', referring to the 'persistent, aggressive cyberspace campaigns' of China and Russia.[76] According to this strategy, the US has sought to enhance resilience and to match the lack of distinction between peacetime and wartime found in China and Russia.[77] Thus, in 2019, USCYBERCOM noted its transition from being a 'response force' to becoming more proactive in countering threats, with the NSA launching its new Cybersecurity Directorate to implement the 2018 cyber strategy of forward-facing continuous engagement in cyberspace.[78]

This proactive strategy aimed to expand interagency, industry and international partner collaboration. It placed US cyber forces alongside air, land, sea and space forces to 'target adversary weaknesses, offset adversary strengths, and amplify the effectiveness of other elements of the joint force', applying 'cyberspace operations across the full spectrum of conflict', under multi-partner, multi-domain, multi-theatre and multi-spectrum operations that have entered into the broader US strategy of 'integrated deterrence'.[79] More recently, the term 'cyber' has been woven throughout

[69] White House, 'Biden–Harris administration delivers on strengthening America's cybersecurity', Fact sheet, 11 Oct. 2022.

[70] US DOD, *National Defense Strategy of the United States of America: Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (US DOD: Washington, DC, 27 Oct. 2022), pp. 8–9.

[71] McGhee, J. E., 'Liberating cyber offense', *Strategic Studies Quarterly*, vol. 10, no. 4 (2016), p. 48.

[72] See e.g. Schoka, A., 'Cyber Command, the NSA, and operating in cyberspace: Time to end the dual hat', *War on the Rocks*, 3 Apr. 2019; see also Pomerleau, 'Key lawmakers in favor of keeping "dual hat" arrangement between Cybercom and NSA' (note 67).

[73] See e.g. Blessing, J. and Harknett, R. J., 'The advantage gained: Building on USCYBERCOM-NSA's "dual hat" synergy model', *Kybernao*, no. 2, Feb. 2022.

[74] US DOD, '2018 DOD cyber strategy and cyber posture review: Sharpening our competitive edge in cyberspace', Fact sheet, 18 Sep. 2018; US DOD, 'Department of Defense Cyber Strategy 2018', Summary sheet, 18 Sep. 2018; and Kollars, N. and Schneider, J., 'Defending forward: The 2018 Cyber Strategy is here', *War on the Rocks*, 20 Sep. 2018.

[75] US DOD, Summary sheet (note 74); Interview with US cyber expert, Washington, DC, 4 Nov. 2022.

[76] US DOD, Fact sheet (note 74).

[77] View of a US expert expressed at the workshop 'Cyber postures and dynamics: China, Russia, United States and Europe' (note 39).

[78] National Security Agency, '2021 NSA cybersecurity year in review', 3 Feb. 2022; and Nakasone, P. M., 'A cyber force for persistent operations', *Joint Force Quarterly*, vol. 92 (Jan. 2019).

[79] US DOD, Summary sheet (note 74).

the US DOD's 2022 versions of the National Defense Strategy, Nuclear Posture Review and Missile Defense Review.[80] This suggests that not only does cyberspace play an integral role throughout US security calculations but also its own territorial dimensions are growing, as evidenced by its explicit pairing in these documents with 'space, air, and undersea domains'.[81]

From zero defect to zero trust

The USA's work to keep pace with rapidly evolving threats and technologies in cyberspace has included a shift from a 'zero defect' strategy to one based on 'zero trust'.[82] The latter recognizes the inevitability of system breach. Thus, the emphasis is not on preventing attacks but rather on preparing for and mitigating the associated consequences as they occur. This demands greater agility, resilience and innovation in defence, achieved through greater engagement of the private sector. To this end, the NSA's Cybersecurity Collaboration Center has a Fusion Operations section that 'teams analysts . . . with industry, academia and government to understand gaps . . . and provide analysis using unclassified resources to solve shared analytic and development challenges'.[83] The Enduring Security Framework, a cross-sector working group supported by the NSA, is a public–private partnership that 'aims to address risks that threaten critical infrastructure and national security systems', such as supply chains.[84] These efforts recognize that the private sector owns and operates the majority of US infrastructure and is often on the frontline. This is also apparent in the Biden administration's focus on critical infrastructure and 'collective resilience' in facing such challenges as ransomware.[85]

Another example of the effort to secure networks of partners and enhance information sharing is Project Indigo, a pilot programme established in 2017 under an agreement between the Financial Services Information Sharing and Analysis Center (FS-ISAC) and USCYBERCOM to share confidential information through a channel known as the Financial Systemic Analysis and Resilience Center (FSARC), itself a subunit of FS-ISAC.[86] Its purpose is allegedly to share cyber threat data, including malware indicators, with USCYBERCOM to help address nation-state hacking aimed at banks. However, the press release of 2016 that announced FSARC's establishment did not mention USCYBERCOM by name—despite describing FSARC's mission as being 'to proactively identify, analyze, assess, and coordinate activities to mitigate systemic risk to the US financial system from current and emerging cybersecurity threats . . . through focused operations and enhanced collaboration between participating firms, industry partners, and government partners'—although it presumably is included in the US 'homeland security, intelligence and defense communities'.[87] This suggests the level of transparency and interoperability among departments continues to have its limits.

[80] US DOD, *National Defense Strategy of the United States of America: Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (note 70).

[81] US DOD, *National Defense Strategy of the United States of America: Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (note 70), pp. 4, 6.

[82] White House, Fact sheet (note 74).

[83] National Security Agency/Central Security Service, 'Fusion operations', [n.d.]; and National Security Agency/Central Security Service, 'NSA Cybersecurity Collaboration Center', [n.d.].

[84] National Security Agency/Central Security Service, 'Enduring Security Framework (ESF)', [n.d.].

[85] White House, Fact sheet (note 74).

[86] Bing, C., 'Inside "Project Indigo": The quiet info-sharing program between banks and US Cyber Command', *CyberScoop*, 21 May 2018.

[87] 'FSARC overview', Federal Reserve Bank of New York, 2016; and Bing (note 86).

From cybersecurity to information security

Despite their differences in tone, both the 2015 and 2018 DOD cyber strategies emphasize an open, free and reliable internet as a foundational objective for US national security. Both accept that while this open internet may increase vulnerabilities, it also creates prosperity and national security advantages. Nevertheless, the year 2015 was a turning point in terms of US views on information security, when the Office of Personnel Management (OPM) data breach, allegedly linked to the Chinese government, compromised approximately 21.5 million records of current, former and prospective federal employees and contractors, spurring a '30-day Cybersecurity Sprint', which has been replicated in multiple follow-on 'sprints' to address ransomware, workforce, industrial control systems, transportation, election security and international collaboration.[88]

Despite these efforts, concerns over information security were compounded during the 2016 presidential election by allegations that Russia had interfered in US electoral processes, resulting in the Department of Homeland Security (DHS) placing election security on its list of critical infrastructure.[89] This issue extended into the 2018 US midterm elections and contributed to the establishment by USCYBERCOM and the NSA of a task force, the Russia Small Group. This task force supported the NSA and USCYBERCOM's Election Security Group in defending the 2020 presidential election against foreign cyberattack. It was reconstituted to address the 2022 midterms and will likely do the same for the 2024 presidential election. In fact, the 2022 US National Defense Strategy's focus on the 'role of information in deterrence', which includes efforts to 'shape perceptions' and engage in 'tailored information operations', suggests that this trend promises to be much more long-term and pervasive.[90]

The Election Security Group directly supports partners like the DHS and the Federal Bureau of Investigation (FBI) in collecting, declassifying and sharing vital information about foreign adversaries to enable domestic efforts in election security. While demonstrating the NSA's foreign intelligence collection and technical expertise and the USCYBERCOM's full-spectrum cyber operations, this cross-departmental process also shows that despite being marginalized with the 2018 expansion of the DOD scope covering critical infrastructure, the DHS and the FBI still play an integral role, as do the private sector and US allies and partners. Such integrative efforts are also reflected in Cyberspace Solarium Commission recommendations that include support for non-governmental disinformation researchers; provision of grants to identify and expose foreign influence campaigns; active DHS and state monitoring of foreign disinformation campaigns; and granting federal authorities power to enforce transparency guidelines for social media platforms.[91] Much of this culminated in the creation of the DHS Disinformation Governance Board in March 2022. However, the pausing of this body three weeks after its creation, followed by its dissolution in August 2022, indicate that USA remains conflicted on how to both define and combat disinformation without entering into censorship.[92]

[88] Scott, T., 'Strengthening and enhancing federal cybersecurity for the 21st century', White House Blog, 31 July 2015; and US Office of Personnel Management (OPM), 'Cybersecurity Resource Center: Cybersecurity incidents', [n.d.].

[89] US Government Accountability Office (GAO), 'DHS plans are urgently needed to address identified challenges before the 2020 elections', Report to congressional committees no. GAO-20-267, Feb. 2020.

[90] US DOD, *National Defense Strategy of the United States of America: Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (note 70), pp. 9, 12–13.

[91] US Cyberspace Solarium Commission, Final report, Mar. 2020.

[92] US Department of Homeland Security, 'Following HSAC Recommendation, DHS terminates Disinformation Governance Board', Press release, 24 Aug. 2022 .

There has also been a US trend towards integrating government and private sector efforts to combat such common threats as ransomware and to pursue investment in quantum computing technology and quantum-resistant cryptography.[93] As an example, in the wake of the Colonial Pipeline cyberattack, the Biden administration issued an executive order intended to improve US cybersecurity and protect government networks, which noted that the private sector must 'adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the federal government to foster a more secure cyberspace'.[94] Nevertheless, firms that operate globally often have competing interests in maintaining their market share, and thus may privilege their customers, shareholders or employees over US national security priorities. This has already played out in criticism over Google's operations in both China and the USA, as well as in fraught efforts by the US DOD to transition to cloud services.[95] The cloud services contract between the DOD and Microsoft, the Joint Enterprise Defense Infrastructure project, was cancelled in 2021, but the DOD has since announced its pursuit of a multi-cloud/multi-vendor contract, the Joint Warfighter Cloud Capability. As the DOD seeks tenders from independent cloud service providers, these firms may also encounter future pressure against military contracts, as occurred already in the artificial intelligence sector with Google.[96]

[93] White House, Fact sheet (note 74).

[94] Denny, W. R., 'Private sector actions in light of the cybersecurity executive order', *Business Law Today*, 13 Sep. 2021; and White House, 'Executive order on improving the nation's cybersecurity', Briefing Room, Presidential Actions, 12 May 2021.

[95] Freedberg Jr, S. J., 'Google helps Chinese military, why not US? Bob Work', *Breaking Defense*, 26 June 2018; and Serbu, J., 'DoD picks Amazon, Microsoft, Google and Oracle for multibillion dollar project to replace JEDI Cloud', Federal News Network, 19 Nov. 2021.

[96] Wakabayashi, D. and Shane, S., 'Google will not renew Pentagon contract that upset employees', *New York Times*, 1 June 2018.

5. The European Union's cyber posture

As a grouping of member states, the EU has faced unique challenges in achieving a unified cyber posture. This is due not only to its structure but also to its limited role in foreign and security policy, where member states cooperate while retaining full sovereignty. As the EU's cyber regulations have expanded exponentially, the term 'cybersecurity' has come to cover a range of concerns, yet reference to 'privacy and data protection' and 'network and information security' remains frequent. While certain member states possess greater capacity than others to shape cybersecurity legislation, the EU has tried to formulate a more cohesive approach. This effort has been led in part by the EU's shift from servicing an internal market to becoming a global provider, as well as collective efforts to formulate tailored responses to cyberattacks through 'limited deterrence by punishment' in the form of sanctions. The names and duties of the key EU organizations in the cyber domain are set out in table 5.1.

From data protection to cybersecurity regulation

In the 1980s, the EU's approach to cybersecurity focused on specific areas such as protection of personal data and the adoption of relevant legislation. In 1981, the Council of Europe passed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which was the first legally binding international instrument in the data protection field.[97] The convention aimed to balance an organization's freedom to use an individual's personal data with protection of the individual's privacy.[98] Notably, this convention ensured the data privacy of European citizens and set the stage for similar EU legislation. By 1995, the EU passed the Data Protection Directive and in 2002 the e-Privacy Directive.[99] The Data Protection Directive was the forerunner of the 2016 General Data Protection Regulation (GDPR), which further expanded the scope and measures of data protection to respond to new technological developments.[100] In particular, the GDPR expanded the definition of 'personal data', provided unified and simpler regulations that are easier for organizations to follow, and implemented non-compliance penalties with a global impact. The security of personal data has thus remained a key pillar of the EU's cybersecurity policy.

An important aspect of protecting personal data relates to combating cybercrime, such as theft of data, which came under specific policies from the late 1990s. The Area of Freedom, Security and Justice (AFSJ) was formally established in 1999 for setting policy agendas on the EU's internal security, including cybercrime policy.[101] Further, the Convention on Cybercrime, adopted by the Council of Europe in 2001, shaped

[97] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), opened for signature 28 Jan. 1981, entered into force 1 Oct. 1985; and Council of Europe, 'Convention 108 and Protocols', [n.d.].

[98] Laperrière, R., Côté, R. and LeBel, G., 'The transborder flow of personal data from Canada: International and comparative law issues', *Jurimetrics*, vol. 32, no. 4 (1992).

[99] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Union*, L281, 23 Nov. 1995; and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal of the European Union*, L201, 31 July 2002.

[100] See Unity, 'The main differences between the DPD and the GDPR and how to address those moving forward', British Legal Technology Forum 2017, Feb. 2017.

[101] European Council, 'The Stockholm Programme—An open and secure Europe serving and protecting citizens', *Official Journal of the European Union*, C115, 4 May 2010.

Table 5.1. Key European Union cyber organizations and their roles and duties

Organization	Role and duties
Computer and Emergency Response Team (CERT-EU)	Hosted within the Directorate-General for Informatics of the European Commission; comprised of information technology experts from EU bodies for the purpose of sharing information, coordinating responses and providing operational assistance
European Cybercrime Centre at Europol (EC3)	Strengthens law enforcement responses to cybercrimes; works as central hub for criminal information and intelligence, supporting criminal investigations; raises awareness of cybercrimes across the EU
European Defence Agency (EDA)	Supports EU member states in developing cyber defence capabilities to improve cyber resilience; works with the EEAS to facilitate exchanges on national cyber defence doctrine, cyber defence-oriented recruitment, retention and reservist programmes
European Union Agency for Cybersecurity (ENISA)	Assists the European Commission and EU member states in meeting the requirements of the Network and Information Security Directive by sharing information and best practices and raising awareness; established an EU-wide cybersecurity certification framework; supports the coordination of the EU response in the case of large-scale, cross-border cyberattacks
European Union External Action Service (EEAS)	Responsible for external EU cybersecurity policy coordination; plays a central role in developing and promoting the EU's core values and strategy in cybersecurity; strengthens international cybersecurity cooperation, especially with NATO
European Union Military Staff (EUMS)	Plays a role in EU cyber defence, supporting development of cyber defence capability of EU member states to ensure protection in military operations

Note: Organizations are listed in English alphabetical order.

the EU's external cybercrime policy.[102] The Stockholm Programme in 2010, the third multi-annual programme on AFSJ policies, highlighted the importance of the 2001 Convention on Cybercrime and the critical role of Europol as 'a European resource centre' that created 'a European platform for identifying offences which should also assist Member States national alert platforms to exchange best practices'.[103] For this purpose, the European Cybercrime Centre was established as a focal point of the EU's fight against cybercrime under the 2013 Directive on Attacks against Information Systems, which was adopted to address the new and emerging channels and methods of cybercrime.[104]

In addition to data protection and cybercrime measures, the EU has launched various initiatives addressing cyber risks in a digital environment, including the 2002 Directive on a Regulatory Framework for Electronic Communications, the 2006 Secure Information Society Strategy and the 2009 Communication on Critical Information

[102] Kasper, A. and Vernygora, V., 'The EU's cybersecurity: A strategic narrative of a cyber power or a confusing policy for a local common market?', *Deusto Journal of European Studies*, no. 65 (Sep. 2021).

[103] European Council, 'The Stockholm Programme—An open and secure Europe serving and protecting citizens' (note 101).

[104] The 2013 version replaced a 2005 version that aimed to improve cooperation between law enforcement and other competent authorities and was a precedent for stricter obligations for EU member states to act against attacks against information systems. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *Official Journal of the European Union*, L218, 14 Aug. 2013. See Hert, P., Fuster, G. and Koops, B., 'Fighting cybercrime in the two Europes: The added value of the EU Framework Decision and the Council of Europe Convention', *Revue internationale de droit Pénal*, vol. 77, nos 3–4 (2006); and Fahey, E., 'The EU's cybercrime and cyber-security rulemaking: Mapping the internal and external dimensions of EU security', *European Journal of Risk Regulation*, vol. 5, no. 1 (2014).

Infrastructure Protection. However, it was not until 2013 that the EU's cybersecurity policy became more unified under the adoption of the first EU Cybersecurity Strategy, which defines cybersecurity as:

> safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.[105]

This strategy addresses five priority areas: 'drastically' reducing cybercrime; achieving cyber resilience, particularly that which is related to network and information security; developing cyber defence capabilities and policy; developing the industrial and technological resources for cybersecurity; and establishing 'a coherent international cyberspace policy' for the EU and promoting core EU values.[106]

In relation to cyber defence as one of the five central strands of the EU's cybersecurity policy, the EU adopted its first Cyber Defence Policy Framework (CDPF) in 2014 under the framework of the EU Common Security and Defence Policy (CSDP).[107] Updated in 2018, the CDPF clarifies the roles of different European actors in cyber defence with the focus on six priority areas, the most important being development of cyber defence capabilities and protection of EU CSDP communication and information networks; the others are training and exercises, research and technology, civil–military cooperation (promoting greater synergies) and international cooperation, specifically with the North Atlantic Treaty Alliance Organization (NATO) and other relevant international partners.[108] The two main organizations driving this development are the European Defence Agency (EDA) and the EU Military Staff (EUMS).

At the same time, amid increasing concerns over state- and non-state-sponsored malicious cyber activities, the EU's cybersecurity policy introduced a more external focus, with the 2017 EU Cyber Diplomacy Toolbox and the EU External Cyber Capacity Building Agenda. The 2020 version of the EU Cybersecurity Strategy expanded its focus to include ensuring a 'global and open Internet' for the 'digital decade'.[109] However, the five priorities in the 2013 EU Cybersecurity Strategy remain the central pillars of the EU's cybersecurity focus. Rather than defining cybersecurity as a 'concept', the strategy uses these five fields to describe its parameters. This explains the determination by the European Union Agency for Cybersecurity (ENISA) that the term 'cybersecurity' is broad and encompasses many facets, making it difficult to formulate a definition that covers its full extent.[110]

[105] Council of the European Union, 'Cybersecurity strategy of the European Union: An open, safe and secure cyberspace', Document no. 52013JC0001, 2013, para. 1.1 note 4. See Dewar, R. S., 'The European Union and cybersecurity: A historiography of an emerging actor's response to a global security concern', M. O'Neill and K. Swinton (eds), *Challenges and Critiques of the EU Internal Security Strategy: Rights, Power and Security'* (Cambridge Scholars: Newcastle-upon-Tyne, 2017), p. 139.

[106] Council of the European Union, 'Cybersecurity strategy' (note 105), para. 2.

[107] Council of the European Union, 'EU Cyber Defence Policy Framework', Document no. 15585/14, 18 Nov. 2014, Annex; and European Union External Action Service, 'The Common Security and Defence Policy', 12 Aug. 2021.

[108] Council of the European Union, 'EU Cyber Defence Policy Framework (2018 update)', Document no. 14413/18, 19 Nov. 2018, Annex, p. 8.

[109] European Commission, 'The EU's cybersecurity strategy for the digital decade', Joint communication to the European Parliament and the Council, 16 Dec. 2020.

[110] European Union Agency for Network and Information Security (ENISA), 'Definition of cybersecurity: Gaps and overlaps in standardisation', Dec. 2015.

From a member state approach to an EU compromise approach

Before the EU came to play a strong centralizing role in cybersecurity in the 2010s, cybersecurity-related matters were under each member state's purview to be dealt with separately. Competing complexities and sensitivities among member states have meant that the EU faces issues with developing a unified cyber posture, as it plays a relatively limited role in foreign and security policy, an area in which 'member states have agreed to cooperate but retain full sovereignty'.[111] These issues include concerns about the extent to which European bodies would or should intervene in the networks of a member state, as well as the effectiveness of handling cybersecurity issues at the EU level, due to a lack of capacity. For example, ENISA—the main EU agency responsible for 'achieving a high common level of cybersecurity across Europe' and whose mandate is ever expanding—consists of only 106 staff members.[112] Additionally, the unanimity requirement and a consensus-seeking culture hinder the EU's decision-making processes, as compromise is required to adopt a decision.[113]

Despite these concerns, there is increasing need for and interest in fostering integrated EU legislation on cybersecurity. The adoption in 2016 of the Network and Information Security Directive (NIS Directive), the first EU-wide legislation on cybersecurity, broke these barriers.[114] The primary aim of the directive is to remove the divergences among national legislation and to synchronize the speed of development in cybersecurity capabilities for protecting critical infrastructure across the different EU member states. Enforcement of the NIS Directive is aimed at eliciting closer coordination and greater confidence among EU member states on cybersecurity issues. More EU legislation on cybersecurity is in development, such as the EU proposal in 2022 of a Cyber Resilience Act to bolster cybersecurity rules through the creation of a shared standard for digital products, including both software and hardware products, to address the vulnerabilities across the EU market.[115]

In the field of cyber defence, the EU has been engaged in developing further initiatives, besides capacity building and information sharing, on collective deterrence and response to cyberattacks. The EU's circumscribed role in security policy means that only limited initiatives are included on the military front in the 2020 EU Cybersecurity Strategy. These include the EU Military Committee's 'Military vision and strategy on cyberspace as a domain of operations' for CSDP military missions and operations, and the setup by the EDA of a Military CERT-Network.[116] Yet these few sections in the strategy do not clearly define the function of the military in cyber defence, much less provide a coherent definition of cyber defence.[117]

From internal market to a global provider

Securing networks and information services for its internal market is one of the main focal points of the EU's cybersecurity policy. The 2019 EU Cybersecurity Act

[111] Archik, K., 'The European Union: Questions and answers', Congressional Research Service Report no. RS21372, 28 Sep. 2022, p. 1.

[112] European Union, 'European Union Agency for Cybersecurity (ENISA)', [n.d.].

[113] Gozi, S., 'Working document on overcoming the deadlock of unanimity voting', Committee on Constitutional Affairs, European Parliament, 28 Apr. 2021.

[114] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *Official Journal of the European Union*, L194, 19 July 2016 (NIS Directive).

[115] European Commission, 'Cyber Resilience Act', 15 Sep. 2022.

[116] European Commission, 'The EU's cybersecurity strategy for the digital decade' (note 109), section 2.4.

[117] Christou, G., *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave Macmillan: London, 2016), p. 139.

provided a framework for European cybersecurity certification schemes that aim to ensure an adequate level of cybersecurity in ICT products, services and processes in the internal market.[118] This is also evident in the 2020 EU Cybersecurity Strategy, in which the building of cyber resilience and an internal market occupies a dominant part. Nevertheless, there are increasing geopolitical tensions that have been linked with cyber issues. The EU's high representative for foreign affairs and security policy, Josep Borrell, highlighted in a 2020 speech that 'cyber issues are geopolitical' and 'the Internet has also become an arena for geopolitical battles'.[119]

The EU's cybersecurity policy has responded to this trend with an increased external focus. The 2020 strategy proposed several initiatives to advance cybersecurity at the international level, including promotion of EU processes in international standardization and norms; expansion of cooperation with partners and the multi-stakeholder community; formation of an informal EU Cyber Diplomacy Network 'to promote the EU vision of cyberspace, exchange information and regularly coordinate on developments in cyberspace'; and strengthening of global resilience through an EU External Cyber Capacity Building Agenda and an EU Cyber Capacity Building Board.[120]

Moreover, the aims of the GDPR in setting standards for data protection at the international level have served as a template for the EU to push for similar initiatives that could also potentially have an impact beyond the EU's borders. For example, the EU Cyber Resilience Act—applying to digital products on the EU's internal market—could become another step towards the EU contributing to international standardization and becoming a regulatory superpower in cyberspace.[121] Regulating a shared standard for digital products that are placed on the EU's internal market will inevitably affect companies based outside the EU that want to keep their access to the market. In this sense, the Cyber Resilience Act could be viewed as a new international standard which may ultimately contribute to the enhancement of global cyber resilience.

From cyber defence to deterrence by denial and limited punishment

Cyber threats within the EU are predominantly addressed by the Foreign Affairs Council, yet there remains a lack of harmonization among units and working groups.[122] The term 'cyber defence' in the EU tends to focus on reducing the incentive for attack by strengthening the resilience of its member states. The EU has launched several initiatives to improve the cybersecurity environment within and beyond the EU, including the NIS Directive and the GDPR to protect critical infrastructure and personal data; the Cybersecurity Act to introduce a cybersecurity certification framework; the EU 5G Toolbox of 2020 to tackle security challenges; and the Cyber Resilience Act to create a shared standard for digital products. Ongoing capacity building, in cooperation with NATO and other international partners, is another key part of the EU's approach.[123]

[118] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act), *Official Journal of the European Union*, L151, 7 June 2019.

[119] Borrell, J., 'Cyber diplomacy and shifting geopolitical landscapes', Speech to the EU Cyber Forum, Brussels, 14 Sep. 2020.

[120] European Commission, 'The EU's cybersecurity strategy for the digital decade' (note 109), sections 3.2–3.3.

[121] Bertuzzi, L., 'Commission expects to set the world's cybersecurity standards for connected devices', Euractiv, 23 Sep. 2022.

[122] Views of European experts expressed at the workshop 'Cyber postures and dynamics: China, Russia, United States and Europe' (note 39).

[123] European Commission, 'The EU's cybersecurity strategy for the digital decade' (note 109).

Despite the gradual buildup of its cyber resilience, the EU remains conflicted on the employment of offensive cyber capabilities. The European Parliament's resolution on the state of EU cyber defence capabilities, adopted in October 2021, recognizes that 'to a certain degree, cyber defence is more effective if it also contains some offensive means and measures'.[124] While this does not automatically equate to a fundamental change in the EU's defence-centric posture, it suggests that there is an evolving approach towards this issue. There are also discussions among EU member states on developing or operating offensive cyber measures or 'hack backs' that would include counterattacks against a cyberattacker.[125]

Instead of fully embracing cyber retaliation, in 2017 the EU proposed punitive measures that involve a sanctions regime and adopted the Cyber Diplomacy Toolbox based on those measures. In May 2019, the EU adopted an autonomous cyber sanctions regime, covering 'substantial elements' of the toolbox, that allows the EU to impose sanctions as a response to cyberattacks.[126] A cyberattack must meet a series of indicators that reach a threshold for a significant threat, before sanctions can be imposed on designated individuals or entities; further, state actors are not included in the scope of this sanctions regime.[127] To demonstrate the viability of the toolbox, the EU imposed sanctions in 2020 on eight individuals and four entities through asset freezes and a travel ban.[128] While the effectiveness of the cyber sanctions regime may be questionable due to the long processing time and limited punitive effect, it demonstrates the determination of the EU to hold individuals and entities behind malicious attacks to account and to signal a unified EU voice.

[124] European Parliament resolution of 7 October 2021 on the state of EU cyber defence capabilities, 2020/2256(INI), Oct. 2021, para. 33.

[125] Herpig, S. and Schuetze, J., 'Transatlantic cyber forum: German government analyses offensive cyber capabilities, so-called "hackbacks"', Stiftung Neue Verantwortung; and Schweighofer, E., Brunner, I. and Zanol, J., 'Malicious cyber operations, "hackbacks" and international law: An Austrian example as a basis for discussion on permissible responses', *Masaryk University Journal of Law and Technology*, vol. 14, no. 2 (2020).

[126] 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; and Council Decision (CFSP) 2019/797796 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.

[127] Council Regulation (EU) 2019/796 (note 126).

[128] European Council, 'Cyber-attacks: Council extends sanctions regime until 18 May 2025', Press release, 16 May 2022.

6. Conclusions

China, Russia, the USA and the EU exhibit a number of convergences and divergences in their cyber posture trends. The most noteworthy trends, and their initial implications for the EU's cyber posture, are outlined below.

Divergence

China and Russia

Following decades of similar trajectories on information security and warfare, China's and Russia's cyber postures have shifted in their priorities. While both have similar concepts of cyber sovereignty and the territoriality of cyberspace, their discourse has begun to diverge. For Russia, while the existence of information-technical operations alongside information-psychological ones suggests that there is a kinetic and cyber warfare component, the terms 'information security' and 'information warfare' continue to dominate official documentation, with a particular focus on psychological warfare and the more recent and expansive 'war against mentality'. By contrast, China's official and unofficial documents have a much more prominent strain of official and unofficial discussion of 'cybersecurity' and 'cyber warfare' and their kinetic consequences. Thus, while the terms 'information security' and 'information warfare' remain prominent in Chinese discourse, China's cyberspace strategies have begun to reflect Western concerns and terminology.

The EU and the USA

The EU and the USA differ in their approaches towards offensive cyber operations. The USA showed indications of such operations as early as 1997, with the NSA's alleged assignment of 'operations to disrupt, deny, degrade or destroy' information in target computers or networks. By 2018, these were codified in the strategies 'defend forward' and 'persistent engagement', which include USCYBERCOM's proactive and daily disruption or halting of malicious cyber activity at its source. By contrast, the EU remains more conflicted on offensive operations and the military use of cyberspace. While the use of offensive measures has been discussed by various EU member states and recognized at the European Parliament level, the EU has focused on imposing sanctions on individuals outside of the cyber domain rather than advocating for pre-emption or full-scale cyber retaliation.

Convergence

Russia and the USA

While long espousing their own versions of deterrence by denial, both Russia and the USA appear to have increasingly shifted towards deterrence by punishment in cyberspace. Following allegations of Russian interference in the 2016 US presidential election, official rhetoric in Russia began to articulate more assertive postures to counter US threats to 'retaliate for the Russia cyberattacks', while Russia's years of alleged cyber activities in Estonia, Georgia and Ukraine demonstrate a punitive and even kinetic direction in cyberspace. As for the USA, its 2010 establishment of USCYBERCOM and its emphasis on 'cost imposition' in both White House and DOD official strategies from both 2018 and 2022 suggest a greater willingness to engage in forward-deployed offensive operations targeting an adversary at its source during tensions or conflict.

China and the USA

Information sharing and collaboration between the government and the private sector remains a work in progress in the USA, in part due to concerns over how data will be used and the military applications of some of these contracts. Nevertheless, the USA is cultivating a more comprehensive and integrated strategy towards cybersecurity. This is reflected not just rhetorically in the consistent reference to the need for a whole-of-government approach, but also in efforts to enhance information sharing and interoperability with the private sector. As part of this, the NSA's Cybersecurity Collaboration Center's Fusion Operations section and its Enduring Security Framework seek to engage universities and the private sector. While the US approach is founded on the ability of civilian-sector entities to decide whether or not to engage on military contracts, these integrative efforts reflect aspects of China's 'military–civil fusion', which also seeks a more holistic approach to strengthen defensive and offensive capabilities.

China, Russia and the USA

China, Russia and the USA are all trending towards more holistic strategies that require a constant cycle of preparation, detection, mitigation, resilience and response to be able to both mitigate and inflict the effects of an electronic 'fog of war'. Even though China and Russia have long shared the term 'active defence', China's concept of 'proactive defence' aligns more closely with the Russian concept of active defence, which is inherently pre-emptive. This growing similarity is important in their similar lack of distinction between peacetime and wartime in cyberspace operations. Thus, what others may perceive as a 'pre-emptive' action is instead viewed within China and Russia as a defensive part of an ongoing conflict. US strategies of 'defend forward' and 'persistent engagement' are similarly embedded in the concept of permanent and protracted conflict, which requires both forward deployment and offensive operations. Furthermore, the USA's official pairing of cyberspace with other domains, such as space, air and undersea, indicates that all three countries exhibit greater convergence when it comes to balancing between defensive and offensive cyber operations and the territorial dimensions of cyberspace.

The EU, the USA, China and Russia

The EU and the USA have long championed freedom in flows of information across the internet, often contrasting their stances with those of China and Russia, which promote cyber sovereignty and non-interference. Nevertheless, the EU's GDPR places an emphasis on data localization and protection, while the USA has also become increasingly focused on information security following the OPM data breach in 2015 and alleged Russian disinformation operations during the 2016 presidential election. The 2022 US National Defense Strategy's focus on the 'role of information in deterrence' is the latest manifestation of this trend. While these shifts do not indicate that the EU and USA are completely aligned with China and Russia, they suggest that all have similar concerns in controlling the flow of information to mitigate the impact of information operations, while also using some of these same techniques to shape their environment. This shift towards both controlling and leveraging information flows is likely to be further reflected in the Biden administration's forthcoming national cybersecurity strategy (yet to be released at the time of writing this).[129]

[129] Curi, M., 'Biden to release national cyber strategy in months (correct)', Bloomberg Law News, 19 Oct. 2022.

Implications for the EU's cyber posture

This overview of cyber posture trends indicates that, while there are a few cases of divergence, China, Russia, the USA and the EU have numerous points of convergence. In seeking ways to engage in crisis management, better understanding of these growing similarities is essential. Such targeted indicators can offer useful insights into how to better understand, anticipate and respond to the other actors' evolving conceptions of the cyber domain, thereby reducing the chances for miscalculation and offering a platform for negotiation.

At the same time, these trends suggest that three of the four actors are heading towards increasingly pre-emptive and confrontational behaviour in cyberspace, while viewing each other as potential adversaries. The EU, which remains conflicted and often the outlier in these dynamics, will have to decide how to formulate its cyber posture to better navigate both its response to and engagement in offensive operations in cyberspace, particularly given the varied stances of its member states.

About the authors

Dr Lora Saalman (United States) is a Senior Researcher within SIPRI's Armament and Disarmament, and Conflict, Peace and Security research areas. She also serves as a Member of the Committee on International Security and Arms Control (CISAC) and as an Adjunct Senior Fellow at the East–West Center (EWC). Her research focuses on China's cyber, nuclear and advanced conventional weapon developments in relation to India, Russia and the USA.

Fei Su (China) is a Researcher with SIPRI's China and Asia Security Programme. Prior to joining SIPRI in 2015 while based in Beijing, she lived and studied in Seoul for three years, achieving fluency in Korean. Her research interests focus on regional security issues in East Asia with a special interest in North Korea, China's foreign and security policy, and maritime security. Her other research interests are within the fields of geo-economics and cybersecurity.

Larisa Saveleva Dovgal (Russia) is a former Intern with the SIPRI Weapons of Mass Destruction Programme. Previously, she worked at the PIR Center in Moscow, focusing on Iran's nuclear programme, China's deterrence capabilities and US nuclear policy. Between January and May 2019, she also worked as Research Assistant at Stockholm University.

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