G7
RESEARCH
GROUP
www.g7.utoronto.ca

2024 G7 Apulia Summit Final Compliance Report

15 June 2024 to 15 May 2025

Prepared by
Jacob Rudolph and Angus MacKellar
and the G7 Research Group
9 June 2025
www.g7.utoronto.ca • g7@utoronto.ca • @g7_rg

"We have meanwhile set up a process and there are also independent institutions monitoring which objectives of our G7 meetings we actually achieve. When it comes to these goals we have a compliance rate of about 80%, according to the University of Toronto. Germany, with its 87%, comes off pretty well. That means that next year too, under the Japanese G7 presidency, we are going to check where we stand in comparison to what we have discussed with each other now. So a lot of what we have resolved to do here together is something that we are going to have to work very hard at over the next few months. But I think that it has become apparent that we, as the G7, want to assume responsibility far beyond the prosperity in our own countries. That's why today's outreach meetings, that is the meetings with our guests, were also of great importance."

Chancellor Angela Merkel, Schloss Elmau, 8 June 2015

G7 summits are a moment for people to judge whether aspirational intent is met by concrete commitments. The G7 Research Group provides a report card on the implementation of G7 and G20 commitments. It is a good moment for the public to interact with leaders and say, you took a leadership position on these issues — a year later, or three years later, what have you accomplished?

Achim Steiner, Administrator, United Nations Development Programme,
in *G7 Canada: The 2018 Charlevoix Summit*

G7 Research Group
University of Toronto
6 Hoskin Avenue, Toronto Ontario M5S 1H6 Canada
g7@utoronto.ca +1-416-946-8953
www.g7.utoronto.ca www.g7g20.utoronto

Contents

20. Cybersecurity: Countering Malicious Behaviour

"We are pursuing a four-fold approach to counter malicious cyber activities … developing and using tools to deter and respond to malicious (State) behavior and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes."

Apulia G7 Leaders' Communiqué

Assessment

	No Compliance	Partial Compliance	Full Compliance
Canada			+1
France			+1
Germany			+1
Italy			+1
Japan			+1
United Kingdom			+1
United States			+1
European Union			+1
Average	+1.00 (100%)		

Background

Countering malicious behaviour within cybersecurity continues to gain momentum within the G7 as technology operates in an increasingly global manner. However, regulation, legislation, and law enforcement mostly remain on the national level.[4642] Cybercrime benefits from gaps in harmonized legislation, creating opportunities for both public and private malicious actors. The topic of the intersection between digital economy and cybersecurity remains relatively novel for G7 leaders. As new, more interdependent, and interrelated technologies began to appear, the development of international recommendations to hold malicious actors accountable emerged. Eventually, the G7 began to address the potential cyber-attacks on the energy sector and increase security on existing digital infrastructure. The 2016 Ise-Shima Summit stands out as it was the first to address cybercrime by both state and non-state actors and responsible state behavior.[4643] At the 2024 Apulia Summit, the G7 recognized that global security continuously depends on transparent, secure, and resilient cyberspaces that respect human rights.[4644] Furthermore, the G7 recognized the importance of cross border cooperation against cybercrime and aims to develop strategies to hold cyber criminals accountable for their actions, thus, committing to working with the G7 Cybersecurity Working Group.[4645] Cyber scams, fraud, extortion, and harassment have led to an increase in cyber incidents targeting valuable information for public and private stakeholders, or to illicitly generate revenue.[4646] In response, G7 leaders have continuously called for increased action, accelerated collaboration, and the creation of tools for stakeholders. Highlights on the G7's governance on cybersecurity follow:

[4642] United Nations Regional Information Centre (Brussels) 4 May 2022. Access Date: 12 September 2024. https://unric.org/en/a-un-treaty-on-cybercrime-en-route/

[4643] G7 Ise-Shima Leaders' Declaration, G7 Information Centre (Toronto) 27 May 2016. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html

[4644] Apulia G7 Leaders' Communiqué, G7 Information Centre (Apulia) 14 June 2024. Access Date: 4 September 2024. https://www.g7.utoronto.ca/summit/2024apulia/240614-apulia-communique.html

[4645] Apulia G7 Leaders' Communiqué, G7 Information Centre (Apulia) 14 June 2024. Access Date: 4 September 2024. https://www.g7.utoronto.ca/summit/2024apulia/240614-apulia-communique.html

[4646] Communiqué, United Nations (New York) 5 September 2024. Access Date: 12 September 2024. https://documents.un.org/doc/undoc/gen/n24/032/68/pdf/n2403268.pdf

At the 1997 Denver Summit, G8 leaders committed to investigating and prosecuting cybercriminals internationally, including providing governments with the technical and legal tools to act against these criminals.[4647]

At the 1998 Birmingham Summit, G8 leaders called for collaboration with the technology industry to work on a legal framework for gathering, disclosing, and protecting data and privacy to tackle crimes against the Internet and other emerging technologies.[4648]

At the 2000 Okinawa Summit, G8 leaders committed to take further action to promote dialogue with the technology industry to address the threat of cybercrime, which was formerly outlined in the Okinawa Charter on Global Information Society.[4649]

At the 2001 Genoa Summit, G8 leaders recognized the importance of judicial collaboration and law enforcement in fighting cybercrime.[4650]

At the 2007 Heiligendamm Summit, G8 leaders committed to developing mechanisms to identify and hinder malicious use of communication and information technology to uncover and eliminate terrorist operations.[4651]

At the 2011 Deauville Summit, G8 leaders recognized the importance of cooperating with governments, regional and international organizations, the private sector, and civil society to counter and sanction the use of information and communications technology (ICT) for terrorism and cybercrime.[4652] Leaders further called for international cooperation against malware and other cyber-attacks on infrastructure, networks, and services, including the Internet.

At the 2015 Elmau Summit, G7 leaders committed to enhancing collaboration to improve energy sector cybersecurity.[4653]

At the 2016 Ise-Shima Summit, G7 leaders committed to use international law against cybercrime by states and non-state actors.[4654] Leaders also encouraged the implementation of voluntary norms to promote trustworthy state activity, denouncing the misuse of ICTs by states for intellectual property crime, including confidential information that could increase its industries' competitiveness. Finally, leaders reaffirmed their commitment to strengthen cybersecurity in the energy sector.

At the 2017 Taormina Summit, G7 leaders called for international cooperation to ensure an open, trustworthy, and safe cyberspace, focusing on countering cyber-attacks on key infrastructure around the world.[4655]

[4647] Communiqué, G7 Information Centre (Toronto) 22 June 1997. Access Date: 2 September 2024. https://www.g7.utoronto.ca/summit/1997denver/g8final.htm

[4648] Communiqué, G7 Information Centre (Toronto) 17 May 1998. Access Date: 2 September 2024. https://www.g7.utoronto.ca/summit/1998birmingham/finalcom.htm

[4649] G8 Communiqué Okinawa 2000, G7 Information Centre (Toronto) 23 July 2000. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2000okinawa/finalcom.htm

[4650] Communiqué, G7 Information Centre (Toronto) 22 July 2001. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2001genoa/finalcommunique.html

[4651] G8 Summit Statement on Counter Terrorism, G7 Information Centre (Toronto) 8 June 2007. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2007heiligendamm/g8-2007-ct.html

[4652] G8 Declaration: Renewed Commitment for Freedom and Democracy, G7 Information Centre (Toronto) 27 May 2011. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2011deauville/2011-declaration-en.html

[4653] Leaders' Declaration: G7 Summit, G7 Information Centre (Toronto) 8 June 2015. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2015elmau/2015-G7-declaration-en.html

[4654] G7 Ise-Shima Leaders' Declaration, G7 Information Centre (Toronto) 27 May 2016. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html

[4655] G7 Taormina Leaders' Communiqué, G7 Information Centre (Toronto) 27 May 2017. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2017taormina/communique.html

At the 2018 Charlevoix Summit, G7 leaders committed to implementing existing international laws and enacting new ones to tackle intellectual property rights cybercrime.[4656]

At the 2021 Cornwall Summit, G7 leaders addressed the importance of ensuring safe and open ICT infrastructure supply chains.[4657] Leaders also committed to guaranteeing the protection of human rights and freedoms by implementing international laws for the use of emerging technologies. Finally, leaders denounced the use of mechanisms that threaten the Group's democratic values such as internet shutdowns and network bans.

At the 2022 Elmau Summit, leaders committed to enhancing the cyber resilience of key digital infrastructure.[4658] Leaders further committed to devising and introducing international cyber laws to ensure responsible state activity in digital spaces. Leaders affirmed their efforts toward improving the Group's cyber defenses against emerging technologies and cybercrime by state and non-state actors. Finally, leaders addressed the need to enforce international laws and assess past efforts for the attribution of cyber cases.

At the 2023 Hiroshima Summit, G7 leaders recognized the importance of collaborating on export controls on key and emerging technologies including digital surveillance instruments to prevent the malicious use of these technologies by ill-intentioned actors.[4659] Leaders also reaffirmed their commitment to tackle transnational organized crime including cybercrime. Leaders welcomed the Budapest Convention on Cybercrime to promote international cooperation for criminal justice. Finally, leaders addressed the importance of safe and resilient cyber infrastructure, endorsing supplier expansion efforts for ICT supply chains.

At the 2024 Apulia Summit, leaders committed to "pursuing a four-fold approach to counter malicious cyber activities ... developing and using tools to deter and respond to malicious (State) behavior and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes."[4660]

Commitment Features

This commitment has six criteria. Two are developing tools and using tools in support of cyber resilience and security. Two criteria are deterring and responding to harmful cyber behaviour that may be carried out by malicious states or cyber criminals. The fifth criterion is disrupting the infrastructure used by malicious states or cyber criminals and the final criterion is enhancing coordination on attributing cyber-attacks to their perpetrators.

Definitions and Concepts

"Attribution process" is understood to mean "the process of tracing and identifying the origin or nature of a cyberattack."[4661]

[4656] The Charlevoix G7 Summit Communiqué, G7 Information Centre (Toronto) 9 June 2018. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2018charlevoix/communique.html

[4657] Carbis Bay G7 Summit Communiqué: Our Shared Agenda for Global Action to Build Back Better, G7 Information Centre (Toronto) 13 June 2021. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2021cornwall/210613-communique.html

[4658] G7 Leaders' Communiqué, G7 Information Centre (Toronto) 28 June 2022. Access Date: 3 September 2024. https://www.g7.utoronto.ca/summit/2022elmau/220628-communique.html

[4659] G7 Hiroshima Leaders' Communiqué, G7 Information Centre (Toronto) 20 May 2023. Access Date: 4 September 2024. https://www.g7.utoronto.ca/summit/2023hiroshima/230520-communique.html

[4660] Apulia G7 Leaders' Communiqué, G7 Information Centre (Apulia) 14 June 2024. Access Date: 4 September 2024. https://www.g7.utoronto.ca/summit/2024apulia/240614-apulia-communique.html

[4661] Cyber attribution, Nord Security (Amsterdam) n.d. Access Date: 2 February 2025. https://nordvpn.com/cybersecurity/glossary/cyber-attribution

"Cyberattack" is understood to mean "an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm."[4662]

"Cybercrime" is understood to mean "criminal activity… committed using a computer especially to illegally access, transmit, or manipulate data."[4663]

"Deter" is understood to mean "to turn aside, discourage, or prevent from acting."[4664]

"Developing" is understood to mean "to gradually become clearer or more detailed."[4665]

"Disrupt" is understood to mean "to interrupt the normal course or unity of [something]."[4666]

"Infrastructure" is understood to mean "the underlying foundation or basic framework (as of a system or organization)."[4667] In the context of this commitment, "cyber infrastructure they use" is understood to mean the physical or digital frameworks used by malicious States or cyber criminals to carry out cyber-attacks.

"Enhancing" is understood to mean "to increase or improve in value, quality, desirability, or attractiveness."[4668]

"Four-fold" is understood to mean having "four units or members."[4669] In the context of this commitment, the four-fold approach refers to the broader G7 commitment to cybersecurity, of which this commitment is one component.[4670]

"Approach" is understood to mean "to make advances to especially in order to create a desired result."[4671]

"Malicious" is understood to mean "having or showing a desire to cause harm to someone: given to, marked by, or arising from malice."[4672]

"State" is understood to mean "a politically organized body of people usually occupying a definite territory."[4673] In the context of this commitment, it refers to the governing authority of this body.

[4662] Cyberattack, Merriam-Webster (Springfield) n.d. Access Date: 12 September 2024. https://www.merriam-webster.com/dictionary/cyberattack

[4663] Cybercrime, Merriam-Webster (Springfield) n.d. Access Date: 12 September 2024. https://www.merriam-webster.com/dictionary/cybercrime

[4664] Deter, Merriam-Webster (Springfield) n.d. Access Date: 12 September 2024. https://www.merriam-webster.com/dictionary/deter

[4665] Developing, Merriam-Webster (Springfield) n.d. Access Date: 12 September 2024. https://www.merriam-webster.com/dictionary/developing

[4666] Disrupt, Merriam-Webster (Springfield) n.d. Access Date: 20 September 2024. https://www.merriam-webster.com/dictionary/disrupt

[4667] Infrastructure, Merriam-Webster (Springfield) n.d. Access Date: 20 September 2024. https://www.merriam-webster.com/dictionary/infrastructure

[4668] Enhancing, Merriam-Webster (Springfield) n.d. Access Date: 12 September 2024. https://www.merriam-webster.com/dictionary/enhancing

[4669] Four-fold, Merriam-Webster (Springfield) n.d. Access Date: 20 September 2024. https://www.merriam-webster.com/dictionary/fourfold

[4670] Apulia G7 Leaders' Communiqué, G7 Information Centre (Apulia) 14 June 2024. Access Date: 2 February 2025. https://www.g7.utoronto.ca/summit/2024apulia/240614-apulia-communique.html

[4671] Approach, Merriam-Webster (Springfield) n.d. Access Date: 20 September 2024. https://www.merriam-webster.com/dictionary/approach

[4672] Malicious, Merriam-Webster (Springfield) n.d. Access Date: 12 September 2024. https://www.merriam-webster.com/dictionary/malicious

[4673] State, Merriam-Webster (Springfield) n.d. Access Date: 20 September 2024. https://www.merriam-webster.com/dictionary/state

"Behaviour" is understood to mean "the way in which something functions or operates."[4674]

"Malicious state behavior," in the context of this commitment, is therefore understood to mean cyber action taken by a foreign government entity intended to cause harm to another entity.

"Pursuing" is understood to mean "to find or employ measures to obtain or accomplish."[4675]

"Respond" is understood to mean "to react in response."[4676]

"Tools" is understood to mean "a means to an end."[4677]

"Using" is understood to mean "to put into action or service: avail oneself of."[4678]

General Interpretive Guidelines

This commitment has six criteria, of which at least four must be addressed strongly in order for the G7 to achieve a score of +1 for full compliance. For partial compliance, or 0, three of the criteria must be met, either by a combination of strong and weak actions, or many weak actions only on three or more of the criteria. For a −1, or no compliance, action was taken two or fewer criteria, or action was taken that was directly and explicitly antithetical to the commitment occurred. Criteria and examples of strong actions are listed in the table below. Example actions may be employed explicitly against state actors, cyber criminals, or to improve general cyber security. Weak actions include verbal reaffirmation of the commitment, expressions of intent of future strong actions, or other actions that do not commit resources to the commitment.

Criteria	Example Actions
Developing tools	Developing and making available programs that private actors can use to test their cyber vulnerabilities; investing in encryption research; forming new agencies or agency branches tasked with fighting cyber crime or enhancing cyber security
Using tools	Launching public information campaigns educating businesses against cyber risks; employing stricter security or encryption practices; testing cyber vulnerabilities of government agencies; increasing funding to agencies or agency branches tasked with fighting cyber crime or enhancing cyber security
Deter malicious cyber activity	Enacting legal changes, such as including cryptocurrencies under anti-money-laundering protections; increasing sentences for cyber criminals; arresting cyber criminals
Respond to malicious cyber activity	Coordinating with international partners to strengthen systems after cyber breaches; issue warnings for private actors using systems that have recently been exploited; information sharing following cyber attacks or anti-cyber crime operations
Disrupt infrastructure	Arresting cyber criminals; conducting asset seizures against cyber criminal organizations; taking down or blocking access to illegal websites or networks
Enhance coordination on attribution processes	Joining joint task forces to fight cyber crime; information sharing or otherwise collaborating on attribution; releasing credible information attributing cyber attacks to various actors using cross-government or transnational coordination

[4674] Behavior, Merriam-Webster (Springfield) n.d. Access Date: 20 September 2024. https://www.merriam-webster.com/dictionary/behavior

[4675] Pursuing, Merriam-Webster (Springfield) n.d. Access Date: 12 September 2024. https://www.merriam-webster.com/dictionary/pursuing

[4676] Respond, Merriam-Webster (Springfield) n.d. Access Date: 12 September 2024. https://www.merriam-webster.com/dictionary/respond

[4677] Tool, Merriam-Webster (Springfield) n.d. Access Date: 20 September 2024. https://www.merriam-webster.com/dictionary/tool

[4678] Using, Merriam-Webster (Springfield) n.d. Access Date: 12 September 2024. https://www.merriam-webster.com/dictionary/using

Scoring Guidelines

−1	The G7 member has taken action in two or fewer criteria: developing tools, using tools, deterring malicious cyber activity, responding to malicious cyber activity, disrupting infrastructure, and enhancing coordination on attribution processes or the G7 member has taken action that is directly and explicitly antithetical to the commitment.
0	The G7 member has taken action in three criteria, including at least one strong action: developing tools, using tools, deterring malicious cyber activity, responding to malicious cyber activity, disrupting infrastructure, and enhancing coordination on attribution processes or the G7 member has taken many weak actions in three or more of the criteria.
+1	The G7 member has taken strong action in at least four of the criteria: developing tools, using tools, deterring malicious cyber activity, responding to malicious cyber activity, disrupting infrastructure, and enhancing coordination on attribution processes.

Compliance Director: Michal Gromek
Lead Analyst: Anali Arambula Galindo

Canada: +1

Canada has fully complied with its commitment to developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes.

On 15 August 2024, the Department of National Defence and the Canadian Armed Forces successfully participated in the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise.[4679] This exercise highlighted Canada's dedication to strengthening cyber defence and interoperability within the North Atlantic Treaty Organization (NATO). Key achievements advanced collaborative cyber defence strategies with seven NATO members, validated new secure network protocols and procedures with Sweden and Romania, and demonstrated a strong capacity to share best practices on a global platform.

On 30 August 2024, Minister of Employment, Workforce Development and Official Languages Randy Boissonnault announced a federal investment of over CAD15.6 million through PrairiesCan for 16 projects across Alberta.[4680] This includes CAD2.3 million to the University of Calgary to create the Canadian Cyber Assessment, Training and Experimentation Centre to encourage cybersecurity solutions and mitigate cyber-attacks among public and private sectors.

On 20 September 2024, Canada, the United Kingdom, and the United States formalized a trilateral agreement to collaborate on cybersecurity and artificial intelligence research.[4681] The initiative focuses on research, development, testing, and evaluation of technologies in artificial intelligence, cyber resilience, and information domain-related areas. It also seeks to utilize previously existing research programs and address new technological challenges on the geopolitical landscape.

On 26 September 2024, Minister of National Defence Bill Blair and Chief of the Defence Staff Jennie Carignan officially announced the establishment of the Canadian Armed Forces Cyber Command.[4682] This new command

[4679] Success at CWIX 2024, Department of National Defence (Ottawa) 15 August 2024. Access Date: 1 November 2024. https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2024/08/success-at-cwix-2024.html

[4680] Minister Boissonnault announces federal investments to commercialize innovative Alberta technologies, Prairies Economic Development Canada (Ottawa) 30 August 2024. Access Date: 1 November 2024. https://www.canada.ca/en/prairies-economic-development/news/2024/08/backgrounder-minister-boissonnault-announces-federal-investments-to-commercialize-innovative-alberta-technologies.html

[4681] UK, US, and Canada to collaborate on cybersecurity and AI research, UK Government (London) 20 September 2024. Access Date: 1 November 2024. https://www.gov.uk/government/news/uk-us-and-canada-to-collaborate-on-cybersecurity-and-ai-research

[4682] Canadian Armed Forces establishes a new cyber command, Department of National Defence (Ottawa) 26 September 2024. Access Date: 1 November 2024. https://www.canada.ca/en/department-national-defence/news/2024/09/canadian-armed-forces-establishes-a-new-cyber-command.html consolidates the Canadian Armed Forces' cyber capabilities into a unified entity, enhancing readiness to address threats in the cyber domain. It also aligns with Canada's commitments to NATO.

On 2 October 2024, Canada joined 67 other members of the International Counter Ransomware Initiative (CRI) in Washington D.C. for the fourth annual CRI Summit.[4683] The summit aimed to improve international cooperation in combating ransomware, and preventing cybercrime across national borders, reflecting Canada's commitment to global cybersecurity collaboration.

On 10 October 2024, G7 Ministers of Industry, Technology, and Digital came together in Rome to discuss digital innovation regarding economic.[4684] One of the key discussions reaffirmed the importance of ethical development in the digital sphere, especially regarding new emerging technologies such as evolving artificial intelligence engines as well as cybersecurity challenges connected with it.

On 29 October 2024, the Canadian Centre for Cyber Security released the Cyber Security Readiness Goals (CRGs).[4685] These goals consist of 36 foundational objectives aimed at improving cybersecurity across Canada's critical infrastructure sectors. The CRGs aim to enhance cyber resilience and minimize potential risks to society, public safety, and the overall stability of the Canadian economy.

On 30 October 2024, the Canadian Centre for Cyber Security released its National Cyber Threat Assessment 2025-2026.[4686] This comprehensive report provides an in-depth analysis of Canada's evolving cyber threat landscape. Within this report, Minister Blair announced CAD917.4 million over five years to enhance intelligence and cyber operations programs, aiming to bolster national security against evolving threats.

On 3 December 2024, the Canadian Center for Cybersecurity and the US Cybersecurity and Infrastructure Security Agency, along with other international agencies, introduced a cybersecurity guidance to enhance protection against global network interferences by foreign state actors.[4687] Specifically, this guidance aims to counter China-sponsored actors.

On 3 December 2024, Canadian officials attended the second meeting of the G7 Cybersecurity Working Group in Rome, aiming to improve coordination between national cybersecurity agencies.[4688] The group focused on harmonizing protections for critical infrastructures, especially in the energy sector, and exploring how artificial intelligence could be used to enhance cybersecurity.

[4683] International Counter Ransomware Initiative 2024 joint statement, Public Safety Canada (Ottawa) 2 October 2024. Access Date: 1 November 2024. https://www.canada.ca/en/public-safety-canada/news/2024/10/international-counter-ransomware-initiative-2024-joint-statement.html

[4684] I ministri dell'Industria e della Technologia del G7 si riuniscono a Roma per promuovere la competitività industrial, l'innovazione digitale e la trasformazione digitale sostenibile, Ministero delle Impresse e del Made in Italy (Rome) 10 October 2024. Translation provided by Google Translate. Access Date: 26 October 2024. https://www.mimit.gov.it/en/media-tools/news/g7-industry-and-technology-ministers-convene-in-rome-to-advance-industrial-competitiveness-digital-innovation-sustainable-digital-transformation

[4685] Cyber Security Readiness Goals: Securing our most Critical Systems, Canadian Centre for Cyber Security (Ottawa) 29 October 2024. Access Date: 1 November 2024. https://www.cyber.gc.ca/en/cyber-security-readiness/cyber-security-readiness-goals-securing-our-most-critical-systems

[4686] Canadian Centre for Cyber Security releases National Cyber Threat Assessment 2025-2026, Canadian Centre for Cyber Security (Ottawa) 30 October 2024. Access Date: 1 November 2024. https://www.canada.ca/en/communications-security/news/2024/10/canadian-centre-for-cyber-security-releases-national-cyber-threat-assessment-2025-2026.html

[4687] Joint guidance on enhanced visibility and hardening for communications infrastructure, Canadian Centre for Cybersecurity (Ottawa) 3 December 2024. Access Date: 17 December 2024. https://www.cyber.gc.ca/en/news-events/joint-guidance-enhanced-visibility-hardening-communications-infrastructure

[4688] Press statement of the President of the G7 Cybersecurity Working Group, Bruno Frattasi, National Cyber Security Agency (Rome) 3 December 2024. Access Date: 19 December 2024. https://www.acn.gov.it/portale/en/w/dichiarazione-alla-stampa-del-presidente-del-gruppo-di-lavoro-g7-sulla-cybersicurezza-bruno-frattasi

On 5 December 2024, the Canadian Centre for Cybersecurity and the Australian Cybersecurity Centre, along with other international collaborators, presented a revised version of the cybersecurity guidance to ensure safety against cyber threats.[4689] This guidance is aimed at assisting private actors to protect themselves from state-sponsored attacks.

On 13 December 2024, Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs Dominic LeBlanc declared Public Safety Canada's funding of CAD10 million for the new Cyber Attribution Data Centre at the Canadian Institute for Cybersecurity at the University of New Brunswick.[4690] This new institution aims to detect cybercriminals and collect information for attribution processes, as well as preparing future cybersecurity professionals.

On 13 January 2025, the Canadian Center for Cyber Security (Cyber Center) joined the United States' Cybersecurity and Infrastructure Agency and other cybersecurity agencies in Europe and Australia to release cybersecurity guidance on securing operation technology (OT) facilities.[4691] The aim of this joint venture is to continue educating OT owners and operators on mechanisms to incorporate security into their device procurement process.

On 16 January 2025, the Treasury Board of Canada Secretariat collaborated with the Cyber Center Learning Hub and Canada School of Public Service Digital Academy to create the Discover Cyber Security course in an effort to protect the Government of Canada's cyber space.[4692] All public servants must take this course to increase their awareness of cyber risks, protecting sensitive information and maintaining operational integrity.

On 4 February 2025, the Cyber Center released joint guidance alongside the French Cyber Security Agency on a risk-based approach to support and secure trusted AI systems and supply chains.[4693] The aim of this venture is to address the rising confidentiality and integrity risks of AI-based systems by suggesting various guidelines such as prohibiting AI-usage to automize critical tasks, as well as monitoring AI systems.

On 4 February 2025, the Cyber Center partnered with other Five Eyes cybersecurity agencies to release a set of publications on cybersecurity for edge devices.[4694] The partners aim to educate on threats to edge devices and encourage the implementation of appropriate measures to circumvent those threats and to facilitate secure connections between networks.

[4689] Executive summary and updated joint guidance on choosing secure and verifiable technologies, Canadian Centre for Cybersecurity (Ottawa) 5 December 2024. Access Date: 17 December 2024. https://www.cyber.gc.ca/en/news-events/executive-summary-and-updated-joint-guidance-choosing-secure-and-verifiable-technologies

[4690] Government of Canada announces financial support for the establishment of a Cyber Attribution Data Centre at the University of New Brunswick, Public Safety Canada (Ottawa) 13 December 2024. Access Date: 18 December 2024. https://www.canada.ca/en/public-safety-canada/news/2024/12/government-of-canada-announces-financial-support-for-the-establishment-of-a-cyber-attribution-data-centre-at-the-university-of-new-brunswick.html

[4691] Joint guidance on secure by demand and priority considerations for operational technology owners and operators when selecting digital products, Canadian Center for Cyber Security (Ottawa) 13 January 2025. Access Date: 7 March 2025. https://www.cyber.gc.ca/en/news-events/joint-guidance-secure-demand-and-priority-considerations-operational-technology-owners-and-operators-when-selecting-digital-products

[4692] New mandatory cyber security course – complete by March 31, 2025, Department of National Defense (Ottawa) 16 January 2025. Access Date: 7 March 2025. https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2025/01/new-mandatory-cyber-security-course.html

[4693] Joint guidance on building trust in artificial intelligence through a cyber risk-based approach, Canadian Center for Cyber Security (Ottawa) 4 February 2025. Access Date: 7 March 2025. https://www.cyber.gc.ca/en/news-events/joint-guidance-building-trust-artificial-intelligence-through-cyber-risk-based-approach#defn-artificial-intelligence

[4694] Five Eyes publish series to sound alarm on cyber security threats to edge devices, Canadian Center for Cyber Security (Ottawa) 4 February 2025. Access Date: 7 March 2025. https://www.cyber.gc.ca/en/news-events/five-eyes-publish-series-sound-alarm-cyber-security-threats-edge-devices#defn-cyber-security

On 6 February 2025, the Government of Canada announced its new National Cyber Security Strategy to protect Canadian cyberspace, position Canada as a leader in global cybersecurity and target cyber threats.[4695] The action plan aims to achieve these goals by deepening partnerships with cybersecurity stakeholders and developing plans to secure continuous investment in Canada's cybersecurity.

On 18 February 2025, the Communications Security Establishment Canada and the Cyber Center released a joint recommendation for Internet-connected OT operators to increase caution against cyber threats.[4696] This targeted recommendation aims to minimize attempts by Russian state cyber operators to exploit exposed OT devices.

On 3 April 2025, the Cyber Center partnered with the US National Security Agency and other international cybersecurity departments to protect private and public networks from fast flux threats.[4697] The cooperation aims to reduce data compromises by adopting network monitoring, machine learning, threat intelligence against fast flux attacks and domain analysis.

On 10 April 2025, the Cyber Center partnered with the United Kingdom's National Cyber Security Centre and cybersecurity agencies from the United States, Australia, Germany and New Zealand to release joint guidance on the spyware variants BADBAZAAR and MOONSHINE.[4698] The publication raised awareness of state-linked cyber threats targeting Uyghur, Tibetan and Taiwanese groups, and provided mitigation measures to help protect high-risk individuals, their devices and their data from surveillance malware.

Canada has fully complied with its commitment to developing and using tools to deter and respond to malicious (state) behavior and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes. Canada has taken strong action to enhance cybersecurity prevention and coordination both on a national and global scale, and has taken strong action towards enhanced coordination on cybercrime attribution processes as well as working towards tools development with investments in cyber research.

Thus, Canada receives a score of +1.

Analysts: Rejaa Khalid and Anali Arambula Galindo

France: +1

France has fully complied with its commitment to developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes.

On 25 June 2024, French judicial authorities participated in a major international anti-cybercrime operation. The operation led to the dismantling of the Coco.gg platform, a hub for the procurement illicit services and materials.[4699]

[4695] Canada's New National Cyber Security Strategy, Canadian Center for Cyber Security (Ottawa) 6 February 2025. Access Date: 7 March 2025. https://www.canada.ca/en/public-safety-canada/news/2025/02/canadas-new-national-cyber-security-strategy.html

[4696] CSE calls on Canadian organizations and critical infrastructure providers to strengthen defences on third anniversary of Russia's invasion of Ukraine, Canadian Center for Cyber Security (Ottawa) 18 February 2025. Access Date: 7 March 2025. https://www.cyber.gc.ca/en/news-events/cse-calls-canadian-organizations-critical-infrastructure-providers-strengthen-defences-third-anniversary-russias-invasion-ukraine

[4697] Joint guidance on fast flux, Canadian Center for Cyber Security (Ottawa) 3 April 2025. Access Date: 8 April 2025. https://www.cyber.gc.ca/en/news-events/joint-guidance-fast-flux#defn-compromise

[4698] Joint guidance on BADBAZAAR and MOONSHINE, Canadian Center for Cyber Security (Ottawa) 9 April 2025. Acxcess Date: 25 April 2025. https://www.cyber.gc.ca/en/news-events/joint-guidance-badbazaar-moonshine

[4699] Major international operation dismantles Coco.gg platform, a hub for illicit activities, Tribunal Judiciaire de Paris (Paris), 25 June 2024. Access Date: 1 March 2025. https://www.tribunal-de-paris.justice.fr/sites/default/files/2024-07/2024-06-25%20-%20CP%20ouverture%20d%27information%20coco.pdf

On 18 July 2024, French judicial authorities launched a disinfection operation, following a report from Sekoia.io in collaboration with Europol. [4700] The operation dismantled the botnet controlled by the PlugX worm, a type of malware that affects digital systems worldwide.

On 17 September 2024, French prosecutors arrested Telegram Chief Executive Officer (CEO) Pavel Durov using France's Orientation and Programming law (LOPMI) legislation, allowing tech titans to be criminally charged based on what occurs on their platforms.[4701] French prosecutors used the law to impose tough sanctions on CEO Durov, which could claim his liability to any illicit actions that are committed on his platform from his users. The implementation of this law will allow a standard to be set to hold responsible those in the technical fields with any criminal activities that occur on their platforms.

On 23 September 2024, France appointed its first Artificial Intelligence (AI) minister Clara Chappaz in Michel Barnier's cabinet as a step towards becoming a global leader in the field of tech.[4702] Minister Chappaz will report to the Ministry of Higher Education and Research regarding all forms of artificial intelligence.

On 10 October 2024, G7 Ministers of Industry, Technology, and Digital came together in Rome to discuss digital innovation regarding economic.[4703] One of the key discussions reaffirmed the importance of ethical development in the digital sphere, especially regarding new emerging technologies such as evolving artificial intelligence engines as well as cybersecurity challenges connected with it.

On November 5, 2024, the State Participations Agency signed a contract to acquire 80% of the capital of Alcatel Submarine Networks (ASN).[4704] ASN manufactures and installs submarine telecom cables. This acquisition demonstrates France's commitment to strengthening its digital sovereignty by acquiring a strategic asset that is essential to the operation of the Internet.

On 25 November 2024, France entered negotiations with Atos, an information technology firm, for the potential acquisition of its advanced computing activities, valued at EUR500 million. The French government aims to retain control over Atos's strategic technology assets, which include securing communications for the military and secret services and manufacturing supercomputers. In doing this, the French government aims to ensure that these cybersecurity capabilities and strategic technologies remain under domestic control, safeguarding national security from external risks or influence.

[4700] Démantèlement du botnet d'espionnage PlugX, Tribunal Judiciaire de Paris (Paris) 24 July 2024. Access Date: 1 March 2025. https://www.tribunal-de-paris.justice.fr/sites/default/files/2024-07/2024-07-24%20-%20CP%20d%C3%A9mant%C3%A8lement%20botnet%20d%27espionnage%20plugX.pdf

[4701] France uses tough, untested cybercrime law to target Telegram's Durov, Reuters (Paris) 17 September 2024. Access Date: 26 October 2024. https://www.reuters.com/world/europe/france-uses-tough-untested-cybercrime-law-target-telegrams-durov-2024-09-17/

[4702] France appoints first AI minister amid political unrest as it aims to become global AI leader, Euro news (Lyon) 23 September 2024. Access Date: 27 October 2024. https://www.euronews.com/next/2024/09/23/france-appoints-first-ai-minister-amid-political-unrest-as-it-aims-to-become-global-ai-lea

[4703] I ministri dell'Industria e della Technologia del G7 si riuniscono a Roma per promuovere la competitività industrial, l'innovazione digitale e la trasformazione digitale sostenibile, Ministero delle Impresse e del Made in Italy (Rome) 10 October 2024. Translation provided by Google Translate. Access Date: 26 October 2024. https://www.mimit.gov.it/en/media-tools/news/g7-industry-and-technology-ministers-convene-in-rome-to-advance-industrial-competitiveness-digital-innovation-sustainable-digital-transformation

[4704] ASN, a strategic manufacturer of submarine telecom cables, nationalized by France, Le Monde (Paris) 5 November 2024. Access Date: 1 March 2025. https://www.lemonde.fr/en/economy/article/2024/11/05/asn-strategic-manufacturer-of-submarine-telecom-cables-nationalized-by-france_6731573_19.html

On 27 November 2024, the Council of Ministers approved a draft law for the establishment of the Cyber Capabilities Development Centre in the Wester Balkans.[4705] The center will focus on strengthening cybersecurity and cooperation, combating cybercrime, and enhancing operational expertise in the region.

On 3 December 2024, French officials attended the second meeting of the G7 Cybersecurity Working Group in Rome, aiming to improve coordination between national cybersecurity agencies.[4706] The group focused on harmonizing protections for critical infrastructures, especially in the energy sector, and exploring how artificial intelligence could be used to enhance cybersecurity.

On 3 December 2024, the French Anti-Cybercrime Office dismantled encrypted messaging service Matrix, in collaboration with Dutch police.[4707] The Franco-Dutch task force had intercepted communications linked to narcotics and arms trafficking prior to the dismantlement.

On 17 December 2024, the Inter-Ministerial Committee at the Archives of France drafted the Interministerial Archives Strategy for 2025-2029, with one of the focuses being on improving the resilience of archives in the face of emerging risks, including cyber-attacks.[4708] This strategy seeks to enhance the security and long-term viability of public archive services through the development of robust digital infrastructure and the strengthening of archive networks.

On 18 December 2024, France's National Cybersecurity Agency (ANSSI) and Germany's Federal Office for Information Security issued a joint report on cybersecurity at major sporting events based on their work securing the 2024 Paris Olympics and the Union of European Football Associations European Football Championship.[4709] The report highlighted preventive and reactive cyber measures implemented in cooperation with the private sector and local stakeholders to prevent disruptions, ensure system resilience and protect event infrastructure amidst heightened geopolitical tensions. This joint effort demonstrated strong international coordination and public-private collaboration to counter cyber threats targeting critical, high-profile events.

On 6 February 2025, the Government of France launched the third phase of its national artificial intelligence strategy, aimed at enhancing collaboration between AI companies and the government.[4710] In alignment with the AI Action Summit, President Emmanuel Macron announced that private companies are expected to invest EUR109 billion over the next few years to support AI in France, including for cybersecurity purposes. France's strategy focuses on strengthening computing infrastructure, leveraging AI to support and train future projects, and transform state ministries to improve public action and increase cybersecurity efficiency.

[4705] Report of the Council of Ministers of November 27, 2024, Government of France (Paris) 28 November 2024, Access Date: 21 December 2024. https://www.info.gouv.fr/conseil-des-ministres/compte-rendu-du-conseil-des-ministres-du-27-11-2024

[4706] Press statement of the President of the G7 Cybersecurity Working Group, Bruno Frattasi, National Cyber Security Agency (Rome) 3 December 2024. Access Date: 19 December 2024. https://www.acn.gov.it/portale/en/w/dichiarazione-alla-stampa-del-presidente-del-gruppo-di-lavoro-g7-sulla-cybersicurezza-bruno-frattasi

[4707] French cyber-gendarmes dismantle the encrypted messaging service Matrix, disrupting high-level organized crime, Le Parisien (Paris) 4 December 2024. Access Date: 1 March 2025. https://www.leparisien.fr/faits-divers/le-haut-du-spectre-de-la-criminalite-organisee-comment-les-cybergendarmes-francais-ont-demantele-la-messagerie-cryptee-matrix-04-12-2024-7CCKP5CHMVG6BK3SGVMYEIOYNE.php

[4708] Interministerial Archives Strategy 2025-2029, Government of France (Paris) 17 December 2024. Access Date: 21 December 2024. https://www.info.gouv.fr/organisation/delegue-et-comite-interministeriel-aux-archives-de-france/strategie-interministerielle-des-archives-2025-2029

[4709] ANSSI and BSI issue a joint release on cybersecurity at major sporting events thanks to cooperation with the private sector, French Cybersecurity Agency (Paris) 06 January 2025. Access Date: 25 April 2025. https://cyber.gouv.fr/en/actualites/anssi-and-bsi-issue-joint-release-cybersecurity-major-sporting-events-thanks-cooperation

[4710] IA: une nouvelle impulsion pour la stratégie nationale, Government of France (Paris) 6 February 2025. Translation provided by Google Translate. Access Date: 8 February 2025. https://www.info.gouv.fr/actualite/ia-une-nouvelle-impulsion-pour-la-strategie-nationale

On 10 February 2025, the Government of France hosted The Global Summit for Action on AI, inviting over 1,500 participants to discuss the role of AI.[4711] During the summit, France promoted the use of AI for France's cybersecurity, national strategy, major scientific advances, education and the workplace, as well as the use of AI in defence and justice.

On 15 April 2025, ANSSI published a set of strategic, operational, and technical guides to support the remediation of cybersecurity incidents.[4712] The guides aim to help organizations contain attacks, restore compromised systems, and improve long-term resilience by providing a doctrinal framework for managing remediation. This initiative contributes to national and sectoral preparedness by strengthening incident response capabilities across the French cybersecurity ecosystem.

France has fully complied with its commitment to developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes. France has invested in developing and using tools to deter, respond to, and disrupt cyberattacks or malicious cyber behavior. This includes implementing strategic policies, fostering international partnerships, and acquiring key technologies to strengthen its cybersecurity infrastructure and ensure national security. Furthermore, towards cybersecurity and the growth of artificial intelligence, it has taken steps to ensure safety and accountability. The usage of the LOPMI legislation sets a precedent that could be utilised in other cybersecurity incidents and challenges such as decentralised cryptocurrency exchanges in the future.

Thus, France receives a score of +1.

Analyst: Zoha Mobeen

Germany: +1

Germany has fully complied with its commitment to developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes.

On 24 July 2024, the Federal Office for Information Security (BSI) approved a draft law to strengthen cybersecurity through the implementation of the EU Directive on Network and Information Security into German law.[4713] This initiative aims to further cybersecurity obligations and reporting in the German private sector and introduces additional regulatory instruments for the BSI.

On 22 August 2024, Federal Minister of the Interior and Community Nancy Faeser conducted a Security Tour across several German regions to discuss the government's initiatives on digital and public security with local public and private stakeholders.[4714] Minister Faeser also discussed government efforts to increase awareness for the cybersecurity area.

On 20 September 2024, the Federal Ministry of the Interior and Community held National Civil Protection Day 2024, focusing on strengthening digital resilience in the face of increasing cyber threats.[4715] This event

[4711] Paris accueille le sommet pour l'action sur l'IA, Government of France (Paris) 10 February 2025. Translation provided by Google Translate. Access Date: 12 February 2025. https://www.info.gouv.fr/actualite/paris-accueille-le-sommet-pour-laction-sur-lia

[4712] ANSSI publishes a set of guides on remediation of cyber incidents, French Cybersecurity Agency (Paris) 15 April 2025. Access Date: 25 April 2025. http://cyber.gouv.fr/en/actualites/anssi-publishes-set-guides-remediation-cyber-incidents

[4713] Stärkung der Cybersicherheit durch EU-Richtlinie NIS-2, Bundesamt für Sicherheit in der Informationstechnik (Berlin) 24 July 2024. Translation provided by Google Translate. Access Date: 1 November 2024. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240724_NIS-2.html

[4714] Sicherheitsreise 2024, Bundesministerium des Innern und für Heimat (Berlin) 15 August 2024. Translation provided by Google Translate. Access Date: 1 November 2024. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/08/sicherheitsreise.html

[4715] Tag des Bevölkerungsschutzes 2024, Bundesministerium des Innern und für Heimat (Berlin) 20 September 2024. Translation provided by Google Translate. Access Date: 1 November 2024. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/09/bevoelkerungsschutztag2024.html centered on enhancing public awareness about cyber resilience and the government's commitment to safeguarding essential services, including healthcare, energy, and transportation, from potential cyber incidents.

On 1 October 2024, the Federal Ministry of the Interior and Community (BMI) launched a range of awareness activities including webinars and workshops within its national coordinator role, during the European Cybersecurity Month.[4716] European Cybersecurity Month is an annual campaign coordinated by European Union Agency for Cybersecurity, with this year's focus being social engineering.

On 10 October 2024, G7 Ministers of Industry, Technology, and Digital came together in Rome to discuss digital innovation regarding economic.[4717] One of the key discussions reaffirmed the importance of ethical development in the digital sphere, especially regarding new emerging technologies such as evolving artificial intelligence engines as well as cybersecurity challenges connected with it.

On 16 October 2024, the BMI signed an agreement with Singapore's Cyber Security Agency to expand cybersecurity labeling between the two nations.[4718] This labelling includes routers in addition to smart consumer devices, furthering international cybersecurity protections between the two countries.

On 18 October 2024, the Federal Ministry of the Interior and Community announced the implementation of the Cyber Resilience Act.[4719] This legislation aims to reinforce cybersecurity standards for digital products across Germany and the European Union. The act introduces a requirement for manufacturers to meet specific cybersecurity criteria, ensuring that products are secure by design before reaching consumers.

On 4 November 2024, the Federal Ministry of Justice released a new draft legislation to increase national cyber resilience.[4720] The proposal aims to introduce legal protection for information technology security researchers who identify and address vulnerabilities in cybersecurity systems. This modifies current laws surrounding unauthorized access, leading to legal uncertainties for professionals working to enhance identify, notify cybersecurity deficiencies. The proposed development would ensure that actions taken with the intention of improving security are no longer penalized under Section 202a of the German Criminal Code.

On 27 November 2024, the BSI, together with 17 EU member states, issued a joint statement requesting public administration and critical infrastructure and industries to embark on a transition towards post-quantum cryptography.[4721] The proposed strategy is concentrating on large-scale fault-tolerant quantum computers, which are to undermine the security of widely used encryption methods by the 2030s.

[4716] Welcome to ECSM, Federal Office for Information Security (Bonn) 1 October 2024. Access Date: 17 December 2024. https://www.bsi.bund.de/EN/Service-Navi/Veranstaltungen/ECSM/ecsm_node.html

[4717] I ministri dell'Industria e della Technologia del G7 si riuniscono a Roma per promuovere la competitività industrial, l'innovazione digitale e la trasformazione digitale sostenibile, Ministero delle Imprese e del Made in Italy (Rome) 10 October 2024. Translation provided by Google Translate. Access Date: 26 October 2024. https://www.mimit.gov.it/en/media-tools/news/g7-industry-and-technology-ministers-convene-in-rome-to-advance-industrial-competitiveness-digital-innovation-sustainable-digital-transformation

[4718] Partnerschaft im Bereich Cybersicherheitskennzeichnung mit Singapur, Bundesamt für Sicherheit in der Informationstechnik (Berlin) 16 October 2024. Translation provided by Google Translate. Access Date: 1 November 2024. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241016_Partnerbehoerde_Singapur_IT-Sik.html

[4719] Cyber Resilience Act, Bundesministerium des Innern und für Heimat (Berlin) 18 October 2024. Translation provided by Google Translate. Access Date: 1 November 2024. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/10/cyber-resilience-act.html

[4720] Rechtssicherheit für die Erforschung von IT-Sicherheitslücken: Bundesjustizministerium veröffentlicht Gesetzentwurf zum Computerstrafrecht, Bundesministerium der Justiz (Berlin) 4 November 2024. Translation provided by Google Translate. Access Date: 17 December 2024. https://www.bmj.de/SharedDocs/Pressemitteilungen/DE/2024/1104_ComputerStrafR.html

[4721] BSI and partners from 17 other EU member states demand transition to Post-Quantum Cryptography, Federal Office for Information Security (Bonn) 27 November 2024. Access Date: 17 December 2024. https://www.bsi.bund.de/EN/Service-Navi/Presse/Pressemitteilungen/Presse2024/241127_Post-Quantum_Cryptography.html

On 29 November 2024, the Federal Office for the Protection of the Constitution established a specialized cybersecurity task force dedicated to addressing cyberattacks, espionage, sabotage, and disinformation campaigns.[4722] The initial triggers were the upcoming German election and the goal to safeguard democratic processes. The task force's objective is to enhance cybersecurity measures, increase resilience against election relate cyber threats and collaborate with transnational partners.

On 3 December 2024, German officials attended the second meeting of the G7 Cybersecurity Working Group in Rome, aiming to improve coordination between national cybersecurity agencies.[4723] The group focused on harmonizing protections for critical infrastructures, especially in the energy sector, and exploring how artificial intelligence could be used to enhance cybersecurity.

On 12 December 2024, the Federal Office for Information Security (BSI) reviewed the European Union's official Cyber Resilience Act, adapting the TR-03183 guideline to increase the efficiency of the legislation.[4724] The BSI's revisions on user surveillance by manufacturers closely aligns with the Cyber Resilience Act by streamlining consumer-oriented standardization in Germany.

On 17 December 2024, the BSI published new security requirements for database systems.[4725] These new requirements address important nodes of the database system, particularly through preset security, hardening, autonomy, logging and interoperability. These changes aim to protect Germany's digital sovereignty by targeting concerns raised by IT administrators, security personnel and federal administrators about the security of their database systems.

On 19 January 2025, the president of the BSI, Claudia Plattner announced the modernization of the IT security specialist certification process in Germany to manage growing demand.[4726] By incorporating third-party accreditations and online assessments, this expansion seeks to ensure cybersecurity concerns are efficiently addressed.

On 21 January 2025, the BSI and Infineon Technologies AG declared a breakthrough in attaining the world's first Common Criteria EAL6 certificate for the implementation of a post-quantum cryptography algorithm in a security controller.[4727] This development counters the growing threats against file and data protections from quantum computers. The leap in the cybersecurity industry is instrumental in ensuring the correct implementation and resistance of IT products from cyberattacks.[4728]

[4722] German task force to tackle foreign meddling before election, Reuters (Berlin) 29 November 2024. Access Date: 17 December 2024. https://www.reuters.com/world/europe/german-task-force-tackle-foreign-meddling-before-election-2024-11-29/

[4723] Press statement of the President of the G7 Cybersecurity Working Group, Bruno Frattasi, National Cyber Security Agency (Rome) 3 December 2024. Access Date: 19 December 2024. https://www.acn.gov.it/portale/en/w/dichiarazione-alla-stampa-del-presidente-del-gruppo-di-lavoro-g7-sulla-cybersicurezza-bruno-frattasi

[4724] Cyber Resilience Act: BSI bewirbt sich um Marktaufsicht für vernetzte Produkt, Bundesamt für Sicherheit in der Informationstechnik (Bonn) 11 December 2024. Translation provided by Google Translate. Access Date: 4 March 2025. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241211_Inkrafttreten-CRA.html

[4725] Neue Sicherheitsanforderungen für Datenbanksysteme veröffentlicht, Bundesamt für Sicherheit in der Informationstechnik (Berlin) 4 March 2025. Translation provided by Google Translate. Access Date: 6 March 2025. https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Sicherheit_Datenbanksysteme_2-250304.html

[4726] Gestiegene Nachfrage: BSI beschleuigt Zertifizierungsverfahren für IT-Sicherheitsdienstleister, Bundesamt für Sicherheit in der Informationstechnik (Bonn) 19 January 2025. Translation provided by Google Translate. Access Date: 4 March 2025. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241219_Zertifizierung_IT-Sicherheitsdienstleister.html

[4727] Erste quantensichere Smartcard zertifiziert, Bundesamt für Sicherheit in der Informationstechnik (Bonn) 21 January 2025. Translation provided by Google Translate. Access Date: 5 March 2025. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250121_erste_quantensichere_Smartcard.html

[4728] Infineon and the BSI pave the way for a quantum-resilient future: World's first Common Criteria Certification for post-quantum cryptography algorithm on a security controller, Infineon Technology (Neubiberg) 23 January 2025. Access Date: 6 March 2025. https://www.infineon.com/cms/en/about-infineon/press/press-releases/2025/INFCSS202501-043.html

On 7 February 2025, the BSI and the Free and Hanseatic City of Hamburg signed an agreement to increase cooperation between the two entities to address cyber crimes in the region.[4729] This agreement is a landmark in federal and state cooperation in addressing growing issues of cyber sabotage and espionage in Germany. These measures target cybersecurity information exchanges, joint awareness-raising measures, advisory services and IT support after security incidents.

On 18 March 2025, the BSI and STACKIT announced the joint development of sovereign cloud solutions for the long-term security of digital products and services.[4730] The cooperation aims to analyze risks and threats to information systems to increase secure usage of public cloud spaces and make German cloud structures more competitive.

On 27 March 2025, State Secretary Markus Richter announced the Government of Germany's new cloud, Deutsche Verwaltungscloud, to secure and standardise cloud services for governmental agencies.[4731] The new cloud system seeks to strengthen the digital sovereignty and security of public administration.

Germany has fully complied with its commitment to developing and using tools to deter and respond to malicious (State) behavior and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes. Germany has implemented a wide range of domestic cybersecurity reforms, passed new legislation to improve digital resilience, and expanded international cooperation through initiatives such as cybersecurity labelling agreements and joint post-quantum cryptography efforts, thus taking strong action towards cybercrime prevention. Germany has also strengthened institutional capacity through new task forces, certification modernization and cloud infrastructure development, strengthening prevention and response capabilities, whilst developing new tools in the field of post-quantum cryptography. Furthermore, Germany has used existing tools to strengthen cybersecurity by adopting and enforcing national cybersecurity standards.

Thus, Germany receives a score of +1.

Analysts: Rejaa Khalid and Michal Gromek

Italy: +1

Italy has fully complied with its commitment to developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes.

On 19 June 2024, Undersecretary of State to the Presidency of the Council of Ministers Alfredo Mantvano stated the Senate's approval of a new government bill on cybersecurity.[4732] The government bill allows for the national security system as well as the cyber sector to have up-to-date equipment and tools to protect from attacks. It will also protect Ital from any future cyber-attacks by focusing on updating its systems as well as strengthening its defenses through collaborations with other governmental groups.

[4729] Cybersicherheit in Bund und Ländern: BSI und Hamburg vereinbaren Kooperation, Bundesamt für Sicherheit in der Informationstechnik (Bonn) 11 February 2025. Translation provided by Google Translate. Access Date: 4 March 2025. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250211_Kooperationsvereinbarung_Hamburg.html

[4730] Cloud Computing: BSI und Schwarz Digits planen Kooperation, Bundesamt für Sicherheit in der Informationstechnik (Bonn) 18 March 2025. Translation provided by Google Translate. Access Date: 6 March 2025. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250318_BSI_Resilienz_Cloud-Loesung.html

[4731] Germany launches government cloud, Federal Ministry of the Interior and Community (Berlin) 27 March 2025. Access Date: 7 March 2025. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2025/03/dvc.html

[4732] Cybersecurity, approvazione definitive del Senato: dichiarazione del Sottosegretario Mantovano, Governo Italiano Persidenza del Consiglio dei Ministri (Rome) 19 July 2024. Translation provided by Google Translate. Access Date: 25 October 2024. https://www.governo.it/it/articolo/cybersecurity-approvazione-definitiva-del-senato-dichiarazione-del-sottosegretario

On 11 September 2024, President of the Campania Region Vincenzo De Luca stated that the Campania Region received EUR14 million in funding to tackle cybersecurity.[4733] The funding was allocated towards information technology security projects in the realm of health services in the region, allowing for constant updates geared towards advancing technologies and maintaining systems to prevent future attacks.

On 10 October 2024, G7 Ministers of Industry, Technology, and Digital came together in Rome to discuss digital innovation regarding economic.[4734] One of the key discussions reaffirmed the importance of ethical development in the digital sphere, especially regarding new emerging technologies such as evolving artificial intelligence engines as well as cybersecurity challenges connected with it.

On 7 November 2024, Prefect Claudio Sgaraglia and the representative of the Italian Banking Association, Marco Laconis signed a memorandum to increase security measures and policies in order to protect the banks and their customers.[4735] This memorandum aims to mitigate the risks of cyber-attacks, robberies and fraud, as well as to prevent financial crimes.

On 21 November 2024, Italy proposed a draft decree aimed at tackling cybercrime by increasing penalties for illegal access to critical systems, including those related to national security and public safety.[4736] The legislation also strengthens the role of the chief anti-mafia prosecutor in overseeing cybercrime investigations.

On 3 December 2024, Italy hosted the second meeting of the G7 Cybersecurity Working Group in Rome, aiming to improve coordination between national cybersecurity agencies.[4737] The group focused on harmonizing protections for critical infrastructures, especially in the energy sector, and exploring how artificial intelligence could be used to enhance cybersecurity.

On 7 February 2025, the National Cybersecurity Agency (ACN) joined a high-level international initiative led by France's cybersecurity agency to address risks associated with artificial intelligence.[4738] The joint analysis, developed with cybersecurity authorities from 15 countries, outlines threats to AI systems and their supply chains and provides recommendations to enhance their security. The initiative supports broader cooperation within the G7 Cybersecurity Working Group and highlights the importance of aligning cybersecurity agencies and AI safety institutions in shaping global approaches to secure and trustworthy AI.

On 12 February 2025, the ACN participated in a high-level meeting in Paris on AI and cybersecurity, held alongside the AI Action Summit and hosted by France's national cybersecurity agency.[4739] The event brought

[4733] De Luca, alla Campania 14 milioni per la Cybersecurity, ANSA it (Salerno) 11 September 2024. Translation provided by Google Translate. Access Date: 25 October 2024. https://www.ansa.it/campania/notizie/giunta_campania/2024/09/11/de-luca-alla-campania-14-milioni-per-la-cybersecurity_1594e059-12ac-4f82-a06b-302c380dc8b2.html

[4734] I ministri dell'Industria e della Technologia del G7 si riuniscono a Roma per promuovere la competitività industrial, l'innovazione digitale e la trasformazione digitale sostenibile, Ministero delle Impresse e del Made in Italy (Rome) 10 October 2024. Translation provided by Google Translate. Access Date: 26 October 2024. https://www.mimit.gov.it/en/media-tools/news/g7-industry-and-technology-ministers-convene-in-rome-to-advance-industrial-competitiveness-digital-innovation-sustainable-digital-transformation

[4735] Protocollo tra prefettura di Milano e Abi per la sicurezza delle banche e dei client, Ministero Dell'Interno (Rome) 7 November 2024. Translation provided by Google Translate. Access Date: 9 November 2024. https://www.interno.gov.it/it/notizie/protocollo-prefettura-milano-e-abi-sicurezza-banche-e-dei-clienti

[4736] Italy plans crackdown on database hacks, Reuters (Rome) 21 November 2024. Access Date: 21 December 2024. https://www.reuters.com/technology/cybersecurity/italy-plans-crackdown-database-hacks-2024-11-21/

[4737] Press statement of the President of the G7 Cybersecurity Working Group, Bruno Frattasi, National Cyber Security Agency (Rome) 3 December 2024. Access Date: 19 December 2024. https://www.acn.gov.it/portale/en/w/dichiarazione-alla-stampa-del-presidente-del-gruppo-di-lavoro-g7-sulla-cybersicurezza-bruno-frattasi

[4738] ACN Joins High-Level Initiative on AI Risks Promoted by French Cyber Agency ANSSI, National Cyber Security Agency (Rome) 7 February 2025. Access Date 25 April 2025. https://www.acn.gov.it/portale/en/comunicazione

[4739] ACN takes part to the AI Summit side event dedicated to cyber agencies in Paris, National Cyber Security Agency (Rome) 12 February 2025. Access Date 25 April 2025. https://www.acn.gov.it/portale/en/w/acn-partecipa-all-incontro-delle-agenzie-cyber-a-margine-dell-ai-summit-di-parigi together 28 agencies, as well as representatives from the EU Commission and other partners. The meeting, which followed a crisis simulation exercise, focused on strengthening cooperation among G7 cyber agencies on securing AI technologies. Participants discussed coordinated strategies for mitigating risks related to AI supply chains and preventing the malicious use of AI systems.

On 18 February 2025, Director General of the ACN Bruno Frattasi met with European Commissioner for Internal Affairs and Migration Magnus Brunner.[4740] The meeting focused on Italy's cybersecurity priorities at the European level, including the implementation of the NIS2 directive and the protection of critical infrastructure. Discussions also covered Italy's engagement in the international Counter Ransomware Initiative and the balance between cybersecurity measures and law enforcement needs. The exchange reinforced Italy's role in advancing coordinated cybersecurity strategies across the European Union.

On 26 February 2025, the ACN held bilateral meetings in Muscat with the Omani Cyber Defence Centre and officials from Oman's Ministry of Foreign Affairs.[4741] The delegation discussed shared cybersecurity priorities and opportunities for cooperation. The visit marked a step forward in strengthening cybersecurity ties between Italy and Oman as part of broader international engagement on digital security.

On 27 February 2025, the ACN adopted national guidelines for implementing the EU Common Criteria (EUCC), the European Union's first cybersecurity certification framework.[4742] The new guidelines define how Italy will authorize and supervise certification bodies, accredit testing laboratories and manage the issuance and oversight of cybersecurity certificates under the EUCC system. This move aligns Italy with EU cybersecurity standards and strengthens national processes for ensuring the security and reliability of digital products and services.

On 28 February 2025, the ACN and the National Agency for the Evaluation of the University and Research System signed a cooperation agreement to strengthen cybersecurity education and research.[4743] The partnership aims to improve coordination between government and academia by tracking national expertise, supporting joint research initiatives and promoting cybersecurity as a strategic academic discipline. The agreement also includes regular reporting on cybersecurity-related research output and aims to foster a national culture of digital security and resilience.

On 5 March 2025, the ACN participated in an EU minister meeting in Warsaw for the first informal Council on Transport, Telecommunications, and Energy fully dedicated to cybersecurity.[4744] The meeting concluded with the unanimous adoption of the Warsaw Declaration, which includes thirteen recommendations to strengthen EU-wide coordination and cyber resilience. Key topics included joint response planning for large-scale cyber incidents, civil-military cooperation and expanding EU funding for cybersecurity.

Italy has fully complied with its commitment to developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes. Italy has taken strong action to strengthen cybersecurity through a bill that will assist in tackling future cyber threats. Additionally, the Italian Cybersecurity Agency has funded initiatives to

[4740] Magnus Brunner at ACN headquarters, National Cyber Security Agency (Rome) 18 February 2025. Access Date 25 April 2025. https://www.acn.gov.it/portale/en/w/magnus-brunner-nella-sede-di-acn

[4741] Ambassador Marotti went to Muscat, National Cyber Security Agency (Rome) 26 February 2025. Access Date 25 April 2025. https://www.acn.gov.it/portale/en/w/visita-ambasciatore-oman

[4742] The national implementation of the EUCC, the first European cybersecurity certification system, is underway, National Cyber Security Agency (Rome) 27 February 2025. Access Date 25 April 2025. https://www.acn.gov.it/portale/en/w/al-via-l-attuazione-nazionale-dell-eucc-il-primo-sistema-europeo-di-certificazione-della-cybersicurezza

[4743] ACN and ANVUR sign a collaboration agreement for the advancement of national cybersecurity, National Cybersecurity Agency (Rome) 28 February 2025. Access Date 25 April 2025. https://www.acn.gov.it/portale/en/w/acn-e-anvur-siglano-un-accordo-di-collaborazione-per-l-avanzamento-della-cybersicurezza-nazionale

[4744] Warsaw: first TTE Council dedicated to cyber security, National Cybersecurity Agency (Rome) 7 March 2025. Access Date 25 April 2025. https://www.acn.gov.it/portale/en/w/varsavia-primo-consiglio-tte-interamente-dedicato-alla-cybersicurezza strengthen the public administration system to ensure that the threats of cyberattacks do not penetrate the system. All these contributions and allocations from the Italian government shows that the country is taking steps towards a safer digital economy while also navigating and learning new artificial intelligence challenges that arise.

Thus, Italy receives a score of +1.

Analyst: Zoha Mobeen

Japan: +1

Japan has fully complied with developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes.

On 16 July 2024, Prime Minister Fumio Kishida, in a meeting with Tuvaluan Prime Minister Feleti Penitala, stated that Japan will provide resources for a submarine cable project in Tuvalu to strengthen the cybersecurity capacity of the country.[4745] This action increases cybersecurity cooperation between countries through the development of infrastructure aimed at deterring malicious cyber activity.

On 17 July 2024, Prime Minister Kishida, during the Japan-Palau Summit, stated Japan's intention of collaborating with Palau on cybersecurity issues, specifically using open Radio Access Network to develop telecommunication network and cyber defense, improving Palau's capacity to detect and respond to threats in cyberspace.[4746] This demonstrates cooperation between countries in enhancing coordination on attribution processes and the implementation of infrastructure made to detect and deter cyberthreats.

On 28 July 2024, Foreign Minister Yoko Kamikawa and Defense Minister Minoru Kihara reaffirmed the importance of cooperation and cyber security in a joint press statement with US Secretary of State Antony Blinken and US Secretary of Defence Lloyd Austin.[4747] This action demonstrates commitment to multinational collaboration on cybersecurity issues.

On 29 July 2024, Foreign Minister Kamikawa met with the Foreign Ministers of Australia and India, as well as the Secretary of State of the United States, where the officials affirmed their commitment to monitoring responsible State behavior in the cyberspace and collaboration on projects such as the International Conference on Cyber Capacity Building in the Philippines and the Quad Cyber Bootcamp in India in the Indo-Pacific region.[4748] They also discussed cooperative efforts in cybersecurity enhancing fields for the protection of critical infrastructure in the Indo-Pacific Region. The final statement demonstrates the countries' commitment to the establishment of a cohesive framework for cybercrime detection and deterrence.

On 5 September 2024, Minister Kamikawa and Minister Kihara, alongside Australian officials, established an Australia-Japan Pacific Development Initiative to develop collaborative connectivity and digital resilience, including telecommunication infrastructure aimed at increasing cybersecurity resilience for Australia and

[4745] Japan-Tuvalu Summit Meeting, Ministry of Foreign Affairs of Japan (Tokyo) 16 July 2024. Access Date: 29 October 2024. https://www.mofa.go.jp/a_o/ocn/tv/pageite_000001_00457.html

[4746] Japan-Palau Summit Meeting, Ministry of Foreign Affairs of Japan (Tokyo) 17 July 2024. Access Date: 29 October 2024. https://www.mofa.go.jp/a_o/ocn/pw/pageite_000001_00469.html

[4747] Secretary Antony J. Blinken, Secretary of Defense Lloyd J. Austin III, Japanese Foreign Minister Kamikawa Yoko, and Japanese Defense Minister Kihara Minoru At a Joint Press Availability, U.S. Department of State (Washington D.C.) 28 July 2024. Access Date: 1 November 2024. https://www.state.gov/secretary-antony-j-blinken-secretary-of-defense-lloyd-j-austin-iii-japanese-foreign-minister-kamikawa-yoko-and-japanese-defense-minister-kihara-minoru-at-a-joint-press-availability/

[4748] Quad Foreign Ministers' Meeting Joint Statement, Ministry of Foreign Affairs of Japan (Tokyo) 29 July 2024. Access Date: 29 October 2024. https://www.mofa.go.jp/files/100704619.pdf

Japan.[4749] This action increases international coordination on cybersecurity efforts via the establishment of an organized framework to counter malicious cyber activity.

On 6 September 2024, Japan, the United States and South Korea held the 3rd Japan-US-ROK Trilateral Diplomacy Working Group for Foreign Ministry Cooperation on North Korea's Cyber Threats in Seoul, where they discussed North Korea's malicious cyber activities which aided in its weapons of mass destruction and ballistic missile programs.[4750] The parties discussed their efforts against these threats as well as cooperative measures, affirming that they will enhance future collaboration adhering to the UN security council's resolutions in the cyber area. This discussion is an example of deterrence and response to malicious state behavior in cyberspace, and the development of coordination between countries against malicious cyber activity.

On 11 September 2024, the Ministry of Foreign Affairs announced that Japan and Lithuania had held their first bilateral meeting on cybersecurity in Vilnius and stated that they would work closely together on cyber issues including strategy, policy, and cooperation through the Japan-Lithuania Bilateral Consultations on Cybersecurity.[4751] This enhances state coordination on cybersecurity, promoting the deterrence of cybercrime and establishing an organized framework.

On 4 October 2024, the Financial Services Agency finalized amendments for the Guidelines for Cybersecurity in the Financial Sector to address the rampant increase of cybersecurity risks over the past few years.[4752] This action further develops a cohesive legislative framework with the purpose of better deterring cybersecurity threats.

On 10 October 2024, G7 Ministers of Industry, Technology, and Digital came together in Rome to discuss digital innovation regarding economic.[4753] One of the key discussions reaffirmed the importance of ethical development in the digital sphere, especially regarding new emerging technologies such as evolving artificial intelligence engines as well as cybersecurity challenges connected with it.

On 10 October 2024, the United States Department of State announced that the US, Australia, India, and Japan were continuing their joint cyber initiative, the Quad Cyber Challenge, aimed at strengthening responsible cyber ecosystems and promoting cybersecurity education and workforce development.[4754] The aim of the joint campaign is to foster education and building a skilled workforce to address emerging cyber threats, supporting the development of future cybersecurity leaders.

On 11 October 2024, Prime Minister Shigeru Ishiba expressed that Japan will be providing connectivity assistance within the Association of Southeast Asian Nations region, allowing members to become better

[4749] Eleventh Australia-Japan 2+2 Foreign and Defense Ministerial Consultations, Ministry of Foreign Affairs of Japan (Tokyo) 5 September 2024. Access Date: 29 October 2024. https://www.mofa.go.jp/files/100720472.pdf

[4750] The 3rd Japan- U.S.-ROK Trilateral Diplomacy Working Group for Foreign Ministry Cooperation on North Korea's Cyber Threats, Ministry of Foreign Affairs of Japan (Tokyo) 6 September 2024. Access Date: 29 October 2024. https://www.mofa.go.jp/press/release/pressite_000001_00575.html

[4751] The 1st Japan-Lithuania Bilateral Consultations on Cybersecurity, Ministry of Foreign Affairs of Japan (Tokyo) 11 September 2024. Access Date: 29 October 2024. https://www.mofa.go.jp/fp/es/pagewe_000001_00091.html

[4752] Publication of the finalized amendments to the "Comprehensive Guidelines for Supervision of Major Banks, etc." and other relevant and applicable Guidelines, alongside the finalized "Guidelines for Cybersecurity in the Financial Sector" (provisional English title) after public consultation, Financial Services Agency (Tokyo) 4 October 2024. Access Date: 29 October 2024. https://www.fsa.go.jp/en/newsletter/weekly2024/607.html

[4753] I ministri dell'Industria e della Technologia del G7 si riuniscono a Roma per promuovere la competitività industrial, l'innovazione digitale e la trasformazione digitale sostenibile, Ministero delle Impresse e del Made in Italy (Rome) 10 October 2024. Translation provided by Google Translate. Access Date: 26 October 2024. https://www.mimit.gov.it/en/media-tools/news/g7-industry-and-technology-ministers-convene-in-rome-to-advance-industrial-competitiveness-digital-innovation-sustainable-digital-transformation

[4754] 2024 Quad Cyber Challenge Joint Statement, U.S. Department of State (Washington D.C.) 21 October 2024. Access Date: 1 November 2024. https://www.state.gov/2024-quad-cyber-challenge-joint-statement/.

connected among themselves with Japan's technological and infrastructural support.[4755] This increases collaboration between members and develops a cohesive framework in cyberspace to better coordinate State response to cybersecurity threats.

On 1 November 2024, Foreign Minister Takeshi Iwaya and High Representative of the European Union for Foreign Affairs and Security Policy and Vice-President of the European Commission Josep Borrell Fontelles announced the Japan-EU Security and Defence Partnership during a strategic dialogue aimed at cooperation in a variety of security issues, one being the enhancement of cybersecurity.[4756] This demonstrates a development of cohesive frameworks between state actors against malicious cyber activity and better coordinated cybersecurity efforts.

On 11 November 2024, the Ministry of Foreign Affairs announced that Japan and the European Union had held a cyber dialogue wherein members discussed cybersecurity strategy, legislation, and infrastructure development to increase bilateral and multilateral cooperation as well as capacity and resilience in the cyber domain.[4757] This exchange demonstrates cooperation between state actors in cyberspace, as well as the establishment of cohesive frameworks for action.

On 12 November 2024, the Ministry of Economy, Trade and Industry announced that the JP-US-EU (Japan – United States – European Union) Industrial Control Systems Cybersecurity Week, including members from the Indo-Pacific Region, had taken place.[4758] This conference gathered experts on cyber defence, infrastructure, and policy, focusing on increasing resilience and state cooperation on the corporate supply chain of digital products. This exchange increases collaboration in international cyber security threats so that state actors may take cooperative measures to increase each other's capacities in the cyber domain.

On 3 December 2024, Japanese officials attended the second meeting of the G7 Cybersecurity Working Group in Rome, aiming to improve coordination between national cybersecurity agencies.[4759] The group focused on harmonizing protections for critical infrastructures, especially in the energy sector, and exploring how artificial intelligence could be used to enhance cybersecurity.

On 9 December 2024, the Government of Japan held a trilateral meeting with the United States and South Korea in Tokyo, where officials announced their Treaty on Comprehensive Strategic Partnership and expressed their commitment to a focused multilateral approach to counter North Korea's malicious cyber activities.[4760] This exchange reinforced international cooperation on cyber security issues, working towards a structured framework amongst state actors.

On 10 January 2025, Prime Minister Ishiba and Malaysian Prime Minister Anwar held a Japan-Malaysia summit where both leaders expressed a desire to increase bilateral cooperation, reaching an agreement on cooperation between the Japan Coast Guard and the Malaysian Maritime Enforcement Agency on issues of national security,

[4755] Press Conference by Prime Minister ISHIBA Shigeru Following His Participation in the ASEAN-related Summit Meetings, Prime Ministers' Office of Japan (Tokyo) 11 October 2024. Access Date: 29 October 2024. https://japan.kantei.go.jp/102_ishiba/statement/202410/1011naigai.html

[4756] Release of the Japan-EU Security and Defence Partnership, Ministry of Foreign Affairs of Japan (Tokyo) 1 November 2024. Access Date: 1 November 2024. https://www.mofa.go.jp/press/release/pressite_000001_00703.html

[4757] The 6th Japan-EU Cyber Dialogue, Ministry of Foreign Affairs of Japan (Tokyo) 11 November 2024. Access Date: 1 December 2024. https://www.mofa.go.jp/press/release/pressite_000001_00728.html

[4758] JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region" Held, Ministry of Economy, Trade and Industry (Tokyo) 15 November 2024. Access Date: 1 December 2024. https://www.meti.go.jp/english/press/2024/1115_001.html

[4759] Press statement of the President of the G7 Cybersecurity Working Group, Bruno Frattasi, National Cyber Security Agency (Rome) 3 December 2024. Access Date: 19 December 2024. https://www.acn.gov.it/portale/en/w/dichiarazione-alla-stampa-del-presidente-del-gruppo-di-lavoro-g7-sulla-cybersicurezza-bruno-frattasi

[4760] Japan-U.S.-ROK Trilateral Meeting on North Korea, Ministry of Foreign Affairs of Japan (Tokyo) 9 December 2024. Access Date: 19 February 2025. https://www.mofa.go.jp/press/release/pressite_000001_00797.html including those of cyber defence.[4761] This action demonstrates coordination between national organization aimed at increased efforts of protecting the cyberspace from possible threats.

On 22 January 2025, the Government of Japan and the Government of the United Kingdom participated in the third Ministerial Japan-UK Digital Council wherein both members reaffirmed the importance of the "Hiroshima Accord: An Enhanced Japan and UK Global Strategic Partnership" to promote collaboration on digital technologies.[4762] This effort affirms the commitment of state actors on collaborative efforts in the digital sphere including cyber resilience efforts.

On 23 January 2025, Ambassador to Cambodia Ueno Atsushi and Cambodian Minister of Foreign Affairs and International Cooperation Prak Sokhonn signed a JPY750 million grant agreement.[4763] Through these funds, Japan will provide cyber security equipment to Cambodia to aid the election process.

On 15 February 2025, Minister of Foreign Affairs Iwaya Takeshi, US Secretary of State Marco Rubio and South Korean Minister of Foreign Affairs Cho Tae-yul attended the Japan-US-Republic of Korea Foreign Ministers' Meeting.[4764] The officials issued a joint statement agreeing to strengthen their cooperation on cyber security deterrence and dedicated response actions, specifically against the malicious cyber activities of North Korea.

On 6 March 2025, the Government of Japan and the Government of Australia held the 6th Japan-Australia Cyber Policy Dialogue in Canberra, where both parties exchanged views on cybersecurity strategy and policy, bilateral and multilateral cooperation and increasing cyber capacity.[4765] Both parties agreed to continue cooperative efforts in the cyberspace. This demonstrates Japan's commitment to collaborative efforts and increased collaboration between state actors against cyber threats.

On 25 March 2025, the Ministry of Economy, Trade and Industry implemented the Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STARI) to ensure any network connecting nonstandard computing hardware or IoT products have appropriate security measures against potential cybercrime.[4766] The JC-STAR scheme mandates standardized cybersecurity labeling for IoT devices based on defined compliance protocols. This initiative reflects Japan's broader commitment to proactive cyber governance through regulatory mechanisms designed to deter cyber threats and increase the security of digital infrastructure.

On 3 April 2025, Minister Iwaya attended the NATO Foreign Ministers' Meeting, reaffirming Japan's commitment to international cyber stability frameworks.[4767] Discussions emphasized alignment with NATO's cyber defense posture, focusing on interoperability, threat intelligence sharing and resilience against state-sponsored cyber threats. This engagement signifies Japan's active role in multilateral cybersecurity enforcement strategies aimed at disrupting transnational cybercrime and malicious digital operations.

On 4 April 2025, the Ministry of Foreign Affairs announced Japan's participation in the 2nd Japan-EU Foreign Ministerial Strategic Dialogue, reinforcing bilateral commitments to cybersecurity cooperation under the Japan-

[4761] Japan-Malaysia Summit Meeting (Summary), Prime Minister's Office of Japan (Tokyo) 10 January 2025. Access Date: 19 February 2025. https://japan.kantei.go.jp/103/diplomatic/202501/10malaysia.html

[4762] UK-Japan Joint Statement: Ministerial Japan-UK digital council January 2025, Ministry of Economy, Trade, and Industry (Tokyo) 22 January 2025. Access Date: 19 February 2025. https://www.soumu.go.jp/main_content/000987609.pdf

[4763] Signing and Exchange of Notes Concerning Grant Aid Project to the Kingdom of Cambodia, Ministry of Foreign Affairs of Japan (Tokyo) 23 January 2025. Access Date: 19 February 2025. https://www.mofa.go.jp/press/release/pressite_000001_00940.html

[4764] Japan-U.S.-ROK Foreign Ministers' Meeting, Ministry of Foreign Affairs of Japan (Tokyo) 15 February 2025. Access Date: 19 February 2025. https://www.mofa.go.jp/a_o/na2/pageite_000001_00001.html

[4765] The 6th Japan-Australia Cyber Policy Dialogue, Ministry of Foreign Affairs of Japan (Tokyo) 7 March 2025. Access Date: 8 April 2025. https://www.mofa.go.jp/press/release/pressite_000001_01064.html

[4766] Launch of IoT Product Security Labeling Scheme (JC-STAR), Ministry of Economy, Trade and Industry (Tokyo) 25 March 2025. Access Date: 8 April 2025. https://www.meti.go.jp/english/press/2025/0325_006.html

[4767] Attendance of Foreign Minister Iwaya at the Meeting of NATO Ministers of Foreign Affairs, Ministry of Foreign Affairs of Japan (Tokyo) 3 April 2025. Access Date: 8 April 2025. https://www.mofa.go.jp/erp/ep/pageite_000001_00004.html

EU Strategic Partnership Agreement.[4768] Key outcomes included coordinated responses to cyberattacks, alignment on norms for responsible state behavior in cyberspace and enhanced joint capacity-building initiatives. This dialogue exemplifies the strengthening of cross-regional cooperation and collaboration in the prevention and mitigation of cyber threats through unified strategic action.

On 9 April 2025, Prime Minister Ishiba and NATO Secretary General Rutte issued a joint statement reaffirming the strategic partnership between Japan and NATO, with a focus on cooperation in cyber defense, space, emerging and disruptive technologies and interoperability.[4769] The leaders emphasized the importance of strengthening collective security and resilience in both the Euro-Atlantic and Indo-Pacific regions. This partnership supports ongoing efforts to coordinate responses to cyber threats and enhance strategic collaboration in the digital domain.

Japan has fully complied with developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes. Japan has taken strong action in the first dimension of the commitment through the development of cybersecurity infrastructure in tandem with other State actors aimed at deterring cyberattacks, establishing rapid response mechanisms, and actively disrupting the infrastructure used by cybercriminals. Further, Japan has taken a multitude of strong and weak actions towards the second dimension of the commitment through collaboration between state actors to accurately deter and identify the sources of cyberattacks via discussion and development of cohesive multi-national frameworks.

Thus, Japan receives a score of +1.

Analyst: Marta Tavares Fernandes

United Kingdom: +1

The United Kingdom has fully complied with its commitment to developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes.

On 17 July 2024, the Department for Science, Innovation, and Technology announced the introduction of the Cyber Security and Resilience Bill, which aims to strengthen the UK's cyber defences and protect essential services from cyberattacks.[4770] The Bill will be introduced in 2025 and will update existing regulations, expand protections for more digital services and supply chains, and require increased incident reporting. It addresses vulnerabilities highlighted by recent attacks on sectors such as the National Health Service and Ministry of Defence, enhancing resilience against cyber threats from state and criminal actors.

On 15 July 2024, Strategic Command announced the occurrence of Exercise Baltic Mule, led by the UK and Poland, aimed to enhance cyber resilience of frontline military forces in Eastern Europe.[4771] The exercise, involving participants from Canada, Estonia, Germany, Latvia, Lithuania, Poland, the UK, and the US, focused on securing military supply lines and communication systems against cyber threats. The exercise supports ongoing efforts to improve military readiness and cyber resilience in the face of increasing cyber threats.

[4768] 2nd Japan-EU Foreign Ministerial Strategic Dialogue, Ministry of Foreign Affairs of Japan (Tokyo) 4 April 2025. Access Date: 8 April 2025. https://www.mofa.go.jp/erp/ep/pageite_000001_00884.html

[4769] Joint Statement H.E. Mr. Ishiba Shigeru, Prime Minister of Japan and H.E. Mr. Mark Rutte, Nato Secretary General, Ministry of Foreign Affairs of Japan (Tokyo) 9 April 2025. Access Date: 25 April 2025. https://www.mofa.go.jp/files/100827718.pdf

[4770] Cyber Security and Resilience Bill, Department for Science, Innovation, and Technology (London) 30 September 2024. Access Date: 30 October 2024. https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

[4771] Improving Cyber Resilience of Frontline Forces in Europe, Strategic Command (London) 15 July 2024. Access Date: 31 October 2024. https://www.gov.uk/government/news/improving-cyber-resilience-of-frontline-forces-in-europe

On 25 July 2024, the Foreign, Commonwealth, & Development Office (FCDO) launched a new "Technology Security Initiative" (TSI) to boost security of telecom networks.[4772] This action enhances cybersecurity by strengthening collaboration on critical and emerging technologies across both parties. It facilitates the identification of priority areas for cyber cooperation and aims to improve cyber resilience through shared efforts in government, research, industry, and academia. The TSI also supports the development of digital technical standards and promotes good internet governance to ensure a secure digital environment.

On 26 July 2024, Secretary of State for Science, Innovation and Technology Peter Kyle announced additional funding of GBP100 million in for five new quantum research hubs.[4773] These hubs will advance secure communication networks, resilient navigation systems, and healthcare innovations, boosting national security and economic growth by developing technologies resistant to cyber threats and improving key sectors.

On 9 August 2024, the Defence Science and Technology Laboratory announced its partnership with the National Quantum Technology Programme and emphasized their work on the integration of artificial intelligence (AI) and data science in the UK's defence and security capabilities.[4774] Their work includes developing AI tools for military use, such as AI-enabled uncrewed vehicles and advanced sensing systems, improving cyber resilience.

On 12 September 2024, Secretary Kyle announced that the Government of the United Kingdom had classified data centres as Critical National Infrastructure (CNI), ensuring greater protection for vital data against cyber threats, outages, and other disruptions.[4775] Additionally, the UK is launching a regional programme to address local cyber skill shortages, investing GBP1.3 million in training and innovation across England and Northern Ireland. This initiative, along with the designation of data centres as CNI, is aimed at strengthening the UK's cyber defenses and encouraging global collaboration to fight cybercrime.

On 16 September 2024, the Department for Science, Innovation, and Technology announced that the UK had hosted global talks with other countries, including the US and EU, to address the rising threat of cyber-attacks.[4776] This will pave the way for a new scheme designed to fill the skills gap by funding cyber training in England and Northern Ireland.

On 20 September 2024, the Department for Science, Innovation, and Technology announced that the UK, in trilateral collaboration with the US and Canada, pursued cyber security measures with the Defence Science and Technology Laboratory as the lead agency.[4777] The parties aim to develop new technologies, methodologies, and tools to tackle real-world challenges, particularly in the cyber and information domains. The partnership

[4772] UK-India Technology Security Initiative factsheet, Foreign, Commonwealth, & Development Office (London) 25 July 2024. Access Date: 31 October 2024. https://www.gov.uk/government/publications/uk-india-technology-security-initiative-factsheet/uk-india-technology-security-initiative-factsheet

[4773] Over £100 million boost to quantum hubs to develop life-saving blood tests and resilient security systems, Department for Science, Innovation, and Technology (London) 26 July 2024. Access Date: 31 October 2024. https://www.gov.uk/government/news/over-100-million-boost-to-quantum-hubs-to-develop-life-saving-blood-tests-and-resilient-security-systems

[4774] AI and data science: defence science and technology capability, Defence Science and Technology Laboratory (London) 15 August 2024. Access Date: 31 October 2024. https://www.gov.uk/guidance/ai-and-data-science-defence-science-and-technology-capability

[4775] Data centres to be given massive boost and protections from cyber criminals and IT blackouts, Department for Science, Innovation, and Technology (London) 12 September 2024. Access Date: 31 October 2024. https://www.gov.uk/government/news/data-centres-to-be-given-massive-boost-and-protections-from-cyber-criminals-and-it-blackouts

[4776] UK Convenes Global Coalition to boost cyber skills and tackle growing threats, Department for Science, Innovation, and Technology (London) 16 September 2024. Access Date: 30 October 2024. https://www.gov.uk/government/news/uk-convenes-global-coalition-to-boost-cyber-skills-and-tackle-growing-threats

[4777] UK, US and Canada to Collaborate on Cybersecurity and AI research, Department for Science, Innovation, and Technology and Ministry of Defense (London) 20 September 2024. Access Date: 30 October 2024. https://www.gov.uk/government/news/uk-us-and-canada-to-collaborate-on-cybersecurity-and-ai-research focuses on projects such as the Cyber Agents for Security Testing and Learning Environments program, which trains AI to defend against cyber threats.

On 1 October 2024, Foreign Secretary David Lammy announced UK sanctions on 16 members of the Russian cyber-crime group Evil Corp.[4778] Led by Maksim Yakubets, the group has been behind numerous cyber-attacks, including malware and ransomware campaigns targeting UK health, government, and private organizations.

On 10 October 2024, G7 Ministers of Industry, Technology, and Digital came together in Rome to discuss digital innovation regarding economic.[4779] One of the key discussions reaffirmed the importance of ethical development in the digital sphere, especially regarding new emerging technologies such as evolving artificial intelligence engines as well as cybersecurity challenges connected with it.

On 23 October 2024, the Department for Science, Innovation and Technology and the National Cyber Security Centre released a joint statement with UK's leading banks to expand the use of Cyber Essentials in supply chain risk management.[4780] The initiative aims to improve cyber resilience across businesses by integrating Cyber Essentials into supplier requirements, raising security standards throughout the UK.

On 23 October 2024, the Central Digital & Data Office laid out a roadmap and strategy for Digital, Data and Technology as part of vision 2025.[4781] As part of this strategy, all digital services and technical infrastructure must be built to comply with the Government Cyber Security Standard, which will ensure efficient, secure and sustainable technology.

On 25 October 2024, Minister of State for Science, Research and Innovation Lord Vallance announced the opening of the National Quantum Computing Centre.[4782] Minister Vallance noted that investment in quantum technology will enhance cybersecurity, providing more secure digital infrastructure and protecting against evolving cyber threats.

On 6 November 2024, the FCDO announced that the UK and Korea had held their fourth Cyber Dialogue in London.[4783] This meeting focused on strengthening bilateral cooperation in cybersecurity, including enhancing coordination on attribution processes and building collective resilience against cyber threats.

On 25 November 2024, the FCDO, the Department for Science Innovation and Technology, Government Communications Headquarters, the Ministry of Defence and the National Cyber Security Centre partnered with the Alan Turing Institute and other organizations to develop advanced cyber defense tools to protect the

[4778] UK sanctions members of notorious 'Evil Corp' cyber-crime gang, after Lammy calls out Putin's mafia state, Foreign, Commonwealth & Development Office (London) 1 October 2024. Access Date: 31 October 2024. https://www.gov.uk/government/news/uk-sanctions-members-of-notorious-evil-corp-cyber-crime-gang-after-lammy-calls-out-putins-mafia-state

[4779] I ministri dell'Industria e della Technologia del G7 si riuniscono a Roma per promuovere la competitività industrial, l'innovazione digitale e la trasformazione digitale sostenibile, Ministero delle Impresse e del Made in Italy (Rome) 10 October 2024. Translation provided by Google Translate. Access Date: 26 October 2024. https://www.mimit.gov.it/en/media-tools/news/g7-industry-and-technology-ministers-convene-in-rome-to-advance-industrial-competitiveness-digital-innovation-sustainable-digital-transformation

[4780] Cyber Essentials Supply Chain Commitment: joint statement, Department for Science, Innovation, and Technology (London) 23 October 2024. https://www.gov.uk/government/publications/cyber-essentials-supply-chain-commitment-joint-statement

[4781] Digital and data function's strategic commitments, Central Digital & Data Office (London) 23 October 2024. Access Date: 31 October 2024. https://www.gov.uk/government/publications/digital-and-technology-spend-control-version-6/c79ccda6-bcd5-495b-88fe-4f1e7824eec9

[4782] New national quantum laboratory to open up access to quantum computing, unleashing a revolution in AI, energy, healthcare and more, Department for Science, Innovation, and Technology (London) 25 October 2024. Access Date: 31 October 2024. https://www.gov.uk/government/news/new-national-quantum-laboratory-to-open-up-access-to-quantum-computing-unleashing-a-revolution-in-ai-energy-healthcare-and-more

[4783] The 4th Republic of Korea-UK Cyber Dialogue Held in London, Foreign, Commonwealth, & Development Office (London) 7 November 2024. Access Date: 16 December 2024. https://www.gov.uk/government/news/the-4th-republic-of-korea-uk-cyber-dialogue-held-in-london

UK's national infrastructure against increasing cyberattacks.[4784] The project is backed by an initial GBP8 million in government funding.

On 3 December 2024, the National Cyber Security Centre published its yearly review.[4785] The report highlighted the rising threat of cyberattacks against the UK, with a focus on state-sponsored threats, data theft, and ransomware. The report mentioned multiple strategies moving forward, such as exploring AI-enhanced cybersecurity solutions to match adversaries' growing capabilities.

On 3 December 2024, UK officials attended the second meeting of the G7 Cybersecurity Working Group in Rome, aiming to improve coordination between national cybersecurity agencies.[4786] The group focused on harmonizing protections for critical infrastructures, especially in the energy sector, and exploring how artificial intelligence could be used to enhance cybersecurity.

On 6 December 2024, the FCDO published details on the second UK-EU Cyber Dialogue in London.[4787] The dialogue covered a range of cybersecurity topics, including cyber resilience, secure technology, digital identity, deterrence strategies against cyber threats, countering cybercrime, and fostering international cooperation for a free, secure cyberspace.

On 8 January 2025, the Department for Science, Innovation and Technology announced that over 30 initiatives across England and Northern Ireland will provide targeted support to strengthen the UK's cyber resilience.[4788] These projects will focus on enhancing protection for businesses and families against potential cyber threats while delivering training programs to develop the nation's cyber skills. The UK government and private sector will allocate a combined GBP1.9 million to fund these initiatives.

On 31 January 2025, the Government of the United Kingdom announced a new code of practice aimed at safeguarding artificial intelligence systems from cyber threats, thereby strengthening the digital economy.[4789] The code is set to serve as the foundation for a new global standard for secure AI through the European Telecommunications Standards Institute, reinforcing the UK's position as a leader in safe innovation.

On 6 February 2025, the Ministry of Defence unveiled a new initiative aimed at rapidly increasing the UK's cyber defence capabilities through a fast-tracked recruitment process.[4790] This program, designed to streamline

[4784] New AI Security Initiative Set to Boost the UK's Resilience against Hostile Threats, The Alan Turing Institute (London) 25 November 2024. Access Date: 16 December 2024. https://www.turing.ac.uk/news/new-ai-security-initiative-set-boost-uks-resilience-against-hostile-threats

[4785] NCSC Annual Review, National Cyber Security Center (London) 3 December 2024. Access Date: 14 December 2024. https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024/chapter-02

[4786] Press statement of the President of the G7 Cybersecurity Working Group, Bruno Frattasi, National Cyber Security Agency (Rome) 3 December 2024. Access Date: 19 December 2024. https://www.acn.gov.it/portale/en/w/dichiarazione-alla-stampa-del-presidente-del-gruppo-di-lavoro-g7-sulla-cybersicurezza-bruno-frattasi

[4787] The second UK-EU Cyber Dialogue takes place in London, Foreign, Commonwealth, & Development Office (London) 6 December 2024. Access Date: 11 December 2024. https://www.gov.uk/government/news/the-second-uk-eu-cyber-dialogue-takes-place-in-london

[4788] New Regional Skills Projects to Bolster UK Cyber Defences and Deliver on Plan for Change, Department for Science, Innovation and Technology (London) 8 January 2025. Access Date: 4 February 2025. https://www.gov.uk/government/news/new-regional-skills-projects-to-bolster-uk-cyber-defences-and-deliver-on-plan-for-change

[4789] World-leading AI Cyber Security Standard to Protect Digital Economy and Deliver Plan for Change, Department for Science, Innovation and Technology (London) 31 January 2025. Access Date: 4 February 2025. https://www.gov.uk/government/news/world-leading-ai-cyber-security-standard-to-protect-digital-economy-and-deliver-plan-for-change

[4790] Fast-track armed forces recruitment launched to boost UK cyber defence, Ministry of Defense (London) 6 February 2025. Access Date: 10 March 2025. https://www.gov.uk/government/news/fast-track-armed-forces-recruitment-launched-to-boost-uk-cyber-defence the entry of skilled individuals into specialist cyber roles, will enable recruits to complete tailored training in just a few weeks. By the end of 2025, successful candidates will be deployed in key operational roles to strengthen the UK's defence against growing cyber threats.

On 11 February 2025, the Government of the United Kingdom, alongside the US and Australia, imposed sanctions on Russian web-hosting provider Zservers and two Russian nationals for supporting LockBit ransomware operations.[4791] The UK government targeted Zservers for providing cybercriminals with servers resistant to law enforcement intervention. The sanctions are part of the UK's broader strategy to combat cybercrime and disrupt criminal infrastructure. British officials also reaffirmed their commitment to working with international partners to dismantle ransomware networks.

On 28 February 2024, the Government of the United Kingdom and the Government of France hosted a high-level conference in London to introduce the Pall Mall Process.[4792] This declaration directly addresses the proliferation and irresponsible use of commercial cyber intrusion tools and services. The meeting brought together international partners and stakeholders to engage in an ongoing dialogue focused on strengthening cybersecurity through enhanced public-private partnerships and multi-stakeholder collaboration.

On 17 March 2025, the Department for Science, Innovation and Technology launched a GBP1.8 million grant competition to support regional cyber security projects across the UK.[4793] Open until 30 April 2025, the programme funds local initiatives focused on developing cyber skills, strengthening local cyber clusters and enhancing community-level resilience.

On 8 April 2025, the Government of the United Kingdom introduced a new Cyber Governance Code of Practice aimed at strengthening cybersecurity leadership across the private sector.[4794] Spearheaded by the Department for Science, Innovation and Technology and the National Cyber Security Centre, the initiative encourages directors and company boards to take greater responsibility for managing cyber risks. The Code outlines clear, actionable measures such as developing cyber strategies, preparing incident response plans and promoting security awareness throughout organizations.

The United Kingdom has fully complied with its commitment to developing and using tools to deter and respond to malicious (State) behavior and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes. The UK has taken strong action to boost data encryption and strength supply chain cybersecurity through the collaboration of the Defense Science and Technology laboratory and the Ministry of Defense, thus contributing both to cybercrime prevention and using tools to prevent cybercrime. The UK has also introduced initiatives and training schemes to fill the skills gap in England and Northern Ireland and allocated funds to boost quantum laboratories and declared data centres as "Critical National Infrastructure," working to develop new tools. Lastly. The UK has countered cybercrime and disrupted criminal infrastructure through sanctioning individuals and entities involved in cybercrime.

Thus, the United Kingdom receives a score of +1.

Analysts: Hajrah Khan Yousafzai and Eleonora Cammarano

[4791] New UK sanctions target Russian cybercrime network, Foreign, Commonwealth & Development Office (London) 11 February 2020. Access Date: 16 February 2025 https://www.gov.uk/government/news/new-uk-sanctions-target-russian-cybercrime-network
[4792] The Pall Mall Process declaration: tackling proliferation and irresponsible use of commercial cyber intrusion capabilities, Foreign, Commonwealth and Development Office (London) 28 February 2025. Access Date: 10 March 2025. https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities
[4793] Funding competition: Cyber Local 2025-2026, Innovation Funding Service (London) 18 March 2025. Access Date: 7 April 2025. https://apply-for-innovation-funding.service.gov.uk/competition/2142/overview/3abce9d2-95e7-4f4e-ab38-b5ee697446f8.
[4794] Business leaders supported to bolster online defences to safeguard growth, Department for Science, Innovation and Technology (London) 8 April 2025. Access Date: 25 April 2025. https://www.gov.uk/government/news/business-leaders-supported-to-bolster-online-defences-to-safeguard-growth

United States: +1

The United States has fully complied with its commitment to developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes.

On 12 June 2024, the Department of State announced that the United States and Spain held their second bilateral Cyber and Digital Dialogue.[4795] During the discussions, both countries reaffirmed their commitment to strengthening cybersecurity and digital policy cooperation, emphasizing the importance of promoting a secure and stable cyberspace, adhering to international law, and supporting the United Nations Cyber Programme of Action.

On 13 June 2024, the Department of State hosted 22 countries and the European Union for discussions on mitigating malicious cyber activity and coordinating global responses.[4796] The talks addressed emerging cybersecurity challenges, including ransomware, foreign interference and emphasizing the importance of adhering to the UN Framework for Responsible State Behavior in Cyberspace.

On 21 June 2024, State Department Spokesperson Matthew Miller released a press reiterating the United States' commitment to safeguarding the integrity of its information and communication technology from cyber threats.[4797] Mr. Miller also announced that the US Department of Commerce had finalized a decision banning Kaspersky Lab and its subsidiaries from providing antivirus software and cybersecurity services within the United States. This action stems from concerns over Kaspersky's cooperation with Russian military and intelligence agencies, which could potentially exploit privileged access granted by its software to compromise U.S. national security.

On 28 July 2024, Secretary of Defense Lloyd Austin reaffirmed the importance of cooperation and cyber security in a joint press statement with Secretary of State Antony Blinken, Japanese Foreign Minister Yoko Kamikawa, and Japanese Defense Minister Minoru Kihara.[4798] This action demonstrates commitment to multinational collaboration on cybersecurity issues.

On 29 July 2024, Secretary of State Antony Blinken met with the Foreign Ministers of Japan, Australia and India, where the officials affirmed their commitment to monitoring responsible State behavior in the cyberspace and collaboration on projects such as the International Conference on Cyber Capacity Building in the Philippines and the Quad Cyber Bootcamp in India in the Indo-Pacific region.[4799] They also discussed cooperative efforts in cybersecurity enhancing fields for the protection of critical infrastructure in the Indo-Pacific Region. The final statement demonstrates the countries' commitment to the establishment of a cohesive framework for cybercrime detection and deterrence.

[4795] Joint Statement on the Second U.S.-Spain Cyber and Digital Dialogue, U.S. Department of State (Washington D.C.) 12 June 2024. Access Date: 1 November 2024. https://www.state.gov/joint-statement-on-the-second-u-s-spain-cyber-and-digital-dialogue/

[4796] Discussions on Deterring Malicious Cyber Activity and the UN Framework of Responsible State Behavior in Cyberspace, U.S. Department of State (Washington D.C.) 17 June 2024. Access Date: 1 November 2024. https://www.state.gov/discussions-on-deterring-malicious-cyber-activity-and-the-un-framework/

[4797] Designating Kaspersky Lab Leadership in Response to Continued Cybersecurity Risks, U.S. Department of State (Washington D.C.) 21 June 2024. Access Date: 1 November 2024. https://www.state.gov/designating-kaspersky-lab-leadership-in-response-to-continued-cybersecurity-risks/

[4798] Secretary Antony J. Blinken, Secretary of Defense Lloyd J. Austin III, Japanese Foreign Minister Kamikawa Yoko, and Japanese Defense Minister Kihara Minoru At a Joint Press Availability, U.S. Department of State (Washington D.C.) 28 July 2024. Access Date: 1 November 2024. https://www.state.gov/secretary-antony-j-blinken-secretary-of-defense-lloyd-j-austin-iii-japanese-foreign-minister-kamikawa-yoko-and-japanese-defense-minister-kihara-minoru-at-a-joint-press-availability/

[4799] Quad Foreign Ministers' Meeting Joint Statement, Ministry of Foreign Affairs of Japan (Tokyo) 29 July 2024. Access Date: 29 October 2024. https://www.mofa.go.jp/files/100704619.pdf

On 16 August 2024, the Department of State announced that senior US and Ukrainian officials had met to convene the US-Ukraine Cyber Dialogue.[4800] Both sides exchanged perspectives on innovation in cybersecurity and communication technology, connectivity and the security and competitiveness of Ukrainian information technology and telecommunications. They also discussed other avenues of cyber assistance to Ukraine, to help uphold its right to self-defence in cyberspace and address longer-term cyber resilience needs.

On 5 September 2024, the United States and Korea convened in Seoul to counter cyber threats posed by North Korea.[4801] The meeting underscored close collaboration to disrupt North Korean cryptocurrency heists, address North Korean cyber espionage against the defense sector and stop third party facilitators from enabling North Korean illicit revenue generation.

On 10 October 2024, the Department of State announced that the US, Australia, India, and Japan were continuing their joint cyber initiative, the Quad Cyber Challenge, aimed at strengthening responsible cyber ecosystems and promoting cybersecurity education and workforce development.[4802] The aim of the joint campaign is to foster education and building a skilled workforce to address emerging cyber threats, supporting the development of future cybersecurity leaders.

On 10 October 2024, G7 Ministers of Industry, Technology, and Digital came together in Rome to discuss digital innovation regarding economic.[4803] One of the key discussions reaffirmed the importance of ethical development in the digital sphere, especially regarding new emerging technologies such as evolving artificial intelligence engines as well as cybersecurity challenges connected with it.

On 18 October 2024, the Biden-Harris Administration launched the Service for America campaign to raise awareness about career opportunities in cybersecurity and make it easier for individuals to access the training and tools needed to enter the field.[4804] The campaign aims to address the mismatch between available cybersecurity jobs and the talent pool by improving the connection between job seekers and employers, thereby strengthening the cybersecurity workforce.

On 18 October 2024, the Department of State announced that the United States and Singapore had conducted a third Cyber Dialogue.[4805] Discussions focused on the regional cybersecurity landscape, including trends in nation-state cyber activity, online fraud, and threats to critical infrastructure. Officials also reviewed progress in bilateral cyber cooperation, cybersecurity policies, and multilateral efforts to build resilience against malicious cyber activity.

On 29 October 2024, the Cybersecurity and Infrastructure Security Agency (CISA) introduced its 2025–2026 International Strategic Plan, designed to enhance collaboration with global partners to protect US critical

[4800] The 2024 U.S.-Ukraine Cyber Dialogue, U.S. Department of State (Washington D.C.) 16 August 2024. Access Date: 1 November 2024. https://www.state.gov/the-2024-u-s-ukraine-cyber-dialogue/

[4801] Seventh United States-Republic of Korea Working Group to Counter Cyber Threats Posed by the Democratic People's Republic of Korea, U.S. Department of State (Washington D.C.) 18 October 2024. Access Date: 1 November 2024. https://www.state.gov/seventh-united-states-republic-of-korea-working-group-to-counter-cyber-threats-posed-by-the-democratic-peoples-republic-of-korea/

[4802] 2024 Quad Cyber Challenge Joint Statement, U.S. Department of State (Washington D.C.) 21 October 2024. Access Date: 1 November 2024. https://www.state.gov/2024-quad-cyber-challenge-joint-statement/.

[4803] I ministri dell'Industria e della Technologia del G7 si riuniscono a Roma per promuovere la competitività industrial, l'innovazione digitale e la trasformazione digitale sostenibile, Ministero delle Impresse e del Made in Italy (Rome) 10 October 2024. Translation provided by Google Translate. Access Date: 26 October 2024. https://www.mimit.gov.it/en/media-tools/news/g7-industry-and-technology-ministers-convene-in-rome-to-advance-industrial-competitiveness-digital-innovation-sustainable-digital-transformation

[4804] Service for America: Cyber Talent is Everywhere and Opportunity Should Be Too, The White House (Washington D.C.) 18 October 2024. Access Date: 1 November 2024. https://www.whitehouse.gov/oncd/briefing-room/2024/10/18/service-for-america-cyber-talent-is-everywhere-and-opportunity-should-be-too/

[4805] Third U.S.-Singapore Cyber Dialogue, U.S. Department of State (Washington D.C.) 5 September 2024. Access Date: 1 November 2024. https://www.state.gov/third-u-s-singapore-cyber-dialogue/

infrastructure by addressing cross-border cybersecurity challenges.[4806] The strategy outlines three core goals aimed at strengthening coordination and tackling the complex risks posed by interconnected cyber and physical systems, emphasizing the need for international cooperation in the face of evolving threats.

On 7 November 2024, Federal agencies submitted updated "zero trust" implementation plans to the White House.[4807] This initiative aims to modernize government cyber defenses by ensuring that no entity inside or outside the network is trusted by default, thereby enhancing the protection of existing cybersecurity frameworks.

On 12 November 2024, the House Homeland Security Committee released a "Cyber Threat Snapshot," highlighting rising threats to US networks and critical infrastructure.[4808] The report emphasized the need for a whole-of-government effort to combat cyber threats from state actors, particularly China, underscoring the importance of coordinated attribution and response efforts.

On 3 December 2024, CISA and the National Security Agency released a guide to help protect communication networks from cyber threats linked to China, who they note have been compromising global telecom networks.[4809] This guide provides steps for network engineers and cybersecurity teams to detect threats, strengthen their networks, and reduce risks of attacks.

On 3 December 2024, US officials attended the second meeting of the G7 Cybersecurity Working Group in Rome, aiming to improve coordination between national cybersecurity agencies.[4810] The group focused on harmonizing protections for critical infrastructures, especially in the energy sector, and exploring how artificial intelligence could be used to enhance cybersecurity.

On 16 December 2024, CISA released the draft update of the National Cyber Incident Response Plan, which serves as the US' strategic framework for coordinating responses to cyber incidents.[4811] CISA emphasized the importance of a unified response framework to keep pace with evolving threats and encouraged public feedback to refine the plan's effectiveness.

On 17 December 2024, CISA introduced Binding Operational Directive 25-01, which aims to enhance the security of cloud services used by federal agencies.[4812] The directive addresses rising cybersecurity risks

[4806] CISA Releases Its First Ever International Strategic Plan, Cybersecurity & Infrastructure Security Agency (Washington D.C.) 29 October 2024. Access Date: 1 November 2024. https://www.cisa.gov/news-events/news/cisa-releases-its-first-ever-international-strategic-plan

[4807] Memorandum for Heads of Executive Departments and Agencies, Executive Office of The President Office of Management and Budget (Washington D.C.) 7 November 2024. Access Date: 16 December 2024. https://www.whitehouse.gov/wp-content/uploads/2024/11/M-25-01-Revised-Circular-A-50.pdf

[4808] NEW: House Homeland Releases 'Cyber Threat Snapshot' Highlighting Rising Threats to US Networks, Critical Infrastructure, Homeland Security Committee (Washington D.C.) 12 November 2024. Access Date: 16 December 2024. https://homeland.house.gov/2024/11/12/new-house-homeland-releases-cyber-threat-snapshot-highlighting-rising-threats-to-us-networks-critical-infrastructure/

[4809] CISA, NSA, FBI and International Partners Publish Guide for Protecting Communications Infrastructure, America's Cybersecurity and Infrastructure Security Agency, 3 December 2024. Access Date 21 December 2024. https://www.cisa.gov/news-events/news/cisa-nsa-fbi-and-international-partners-publish-guide-protecting-communications-infrastructure

[4810] Press statement of the President of the G7 Cybersecurity Working Group, Bruno Frattasi, National Cyber Security Agency (Rome) 3 December 2024. Access Date: 19 December 2024. https://www.acn.gov.it/portale/en/w/dichiarazione-alla-stampa-del-presidente-del-gruppo-di-lavoro-g7-sulla-cybersicurezza-bruno-frattasi

[4811] CISA Publishes Draft National Cyber Incident Response Plan for Public Comment, America's Cybersecurity and Infrastructure Security Agency, 16 December 2024. Access Date 21 December 2024. https://www.cisa.gov/news-events/news/cisa-publishes-draft-national-cyber-incident-response-plan-public-comment

[4812] CISA Directs Federal Agencies to Secure Cloud Environments, America's Cybersecurity and Infrastructure Security Agency, 17 December 2024. Access Date 21 December 2024. https://www.cisa.gov/news-events/news/cisa-directs-federal-agencies-secure-cloud-environments associated with cloud misconfigurations, which are vulnerable to exploitation by cybercriminals seeking unauthorized access or data breaches. By enforcing this directive, CISA seeks to minimize risks and bolster the defense posture of the federal government's network infrastructure.

On 17 December 2024, CISA released a new guide titled "Playbook for Strengthening Cybersecurity in General Grant Programs for Critical Infrastructure."[4813] The guide is designed to help grant-making agencies incorporate cybersecurity into their funding programs.

On 3 January 2025, the Department of the Treasury's Office of Foreign Assets Control imposed sanctions on Integrity Technology Group (ITG), a Beijing-based cybersecurity company.[4814] The sanctions responded to ITG's involvement aiding Flax Typhoon, a Chinese state-sponsored cyber group responsible for multiple attacks on U.S. entities.

On 30 January 2025, the Department of Justice announced the coordinated seizure of 39 domains associated with a Pakistan-based network of online marketplaces selling hacking and fraud-enabling tools operated by a group known as Saim Raza (also known as HeartSender).[4815] This international operation aimed to disrupt the sale of hacking tools and stolen data.

On 11 February 2025, the Department of the Treasury announced that the US, in coordination with the UK and Australia, had imposed sanctions on Russian web-hosting provider Zservers and two Russian nationals for supporting the ransomware group LockBit.[4816] This action aimed to disrupt infrastructure facilitating ransomware attacks on critical infrastructure globally.

On 26 February 2025, the House Committee on Homeland Security unanimously advanced the Cyber PIVOTT Act of 2025, a bill to expand cybersecurity education and workforce development.[4817] The committee also adopted its oversight plan for the 119th Congress, emphasizing protection of critical infrastructure and Department of Homeland Security (DHS) cyber initiatives.

On 5 March 2025, the Government of the United States announced a crackdown on Chinese cyber-espionage.[4818] The Justice Department unsealed indictments against ten Chinese nationals linked to a years-long hacking campaign targeting US government agencies and foreign ministries. The Treasury Department sanctioned a Chinese firm and its owner for trafficking in stolen US data, while it offered a USD10 million reward for information on the suspects.

On 3 April 2025, CISA, the National Security Agency, the Federal Bureau of Investigation and cybersecurity agencies from Australia, Canada and New Zealand released a joint advisory highlighting the use of fast-flux

[4813] CISA and ONCD Publish Guide to Strengthen Cybersecurity of Grant-Funded Infrastructure Projects, America's Cybersecurity and Infrastructure Security Agency, 17 December 2024. Access Date 21 December 2024. https://www.cisa.gov/news-events/news/cisa-and-oncd-publish-guide-strengthen-cybersecurity-grant-funded-infrastructure-projects

[4814] Treasury Sanctions Technology Company for Support to Malicious Cyber Group, U.S. Department of the Treasury, 3 January 2025. Access Date 11 May 2025. https://home.treasury.gov/news/press-releases/jy2769

[4815] Justice Department Announces Seizure of Cybercrime Websites Selling Hacking Tools to Transnational Organized Crime Groups, U.S. Department of Justice Office of Public Affairs (Washington D.C.) 30 January 2025. Access Date: 15 February 2025. https://www.justice.gov/opa/pr/justice-department-announces-seizure-cybercrime-websites-selling-hacking-tools-transnational

[4816] United States, Australia, and the United Kingdom Jointly Sanction Key Infrastructure that Enables Ransomware Attacks, U.S. Department of the Treasury (Washington D.C.) 11 February 2025. Access Date: 15 February 2025. https://home.treasury.gov/news/press-releases/sb0018

[4817] Committee Advances 'Cyber PIVOTT Act,' Adopts 119th Congress Oversight Plan, Homeland Security Committee (Washington D.C.) 26 February 2025. Access Date: 8 April 2025. https://homeland.house.gov/2025/02/26/committee-advances-cyber-pivott-act-adopts-119th-congress-oversight-plan/

[4818] US Indicts Slew of Alleged Chinese Hackers, Sanctions Company over Spy Campaign, Reuters (Washington D.C.) 6 March 2025. Access Date: 8 April 2025. https://www.reuters.com/technology/us-indicts-slew-alleged-chinese-hackers-sanctions-company-over-spy-campaign-2025-03-05/

techniques by cybercriminals.[4819] The advisory warned of growing risks associated with rapidly shifting DNS records and urged defenders to improve detection and mitigation strategies.

On 23 April 2025, CISA and the DHS led a joint training exercise with energy sector partners to improve cyber response in critical infrastructure.[4820] The simulation involved real-time OT and IT attack scenarios. The exercise helped participants strengthen their skills in detecting and managing cyber threats, highlighting ongoing efforts to build national resilience and technical capacity.

On 23 April 2025, the Government of the United States reaffirmed its support for the Common Vulnerabilities and Exposures Program, clarifying that recent concerns about a funding lapse were unfounded[4821]. CISA emphasized its ongoing leadership role in maintaining and expanding the program, which enables faster identification and disclosure of cybersecurity vulnerabilities through a global network of over 450 partners. The statement reinforced the program's value in supporting timely threat response and strengthening international cybersecurity coordination.

The United States has fully complied with its commitment to developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes. The State Department has focused on bilateral agreements with international partners and voiced support for cybersecurity measures in accordance with the United Nations framework of Responsible State Behaviour in Cyberspace. Furthermore, the United States has taken strong action towards both developing advanced technologies to counter malicious cyber behavior and enhancing coordination efforts to identify attackers. This includes ongoing initiatives to strengthen cybersecurity tools, collaborate with international partners, and improve the detection and attribution of cyber threats.

Thus, the United States receives a score of +1.

Analysts: Hajrah Khan Yousafzai and Eleonora Cammarano

European Union: +1

The European Union has fully complied with their commitment to developing and using tools to deter and respond to malicious behaviour and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes.

On 15 July 2024, the European Union and Ukraine conducted a cyber-dialogue in Brussels where they agreed to increased international cooperation on cybersecurity and diplomacy issues to promote responsible state behaviour in cyberspace.[4822] Both parties discussed efforts regarding the prevention and deterrence of malicious cyber activities through the use of the EU Cyber Diplomacy Toolbox and Cyber Sanctions Regime, as well as the strengthening of critical infrastructure. This demonstrates a commitment to international collaboration in cyberspace, promoting an organized framework against potential cyberthreats.

On 6 September 2024, EU Cybernet experts facilitated a four-day Cyber Incidents Response Training at the Central Bank of Lesotho to enhance the banks' security capabilities against cyber-attacks and strengthen

[4819] Fast Flux: A National Security Threat, Cybersecurity and Infrastructure Security Agency (Washington D.C.) 3 April 2025. Access Date: 8 April 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-093a

[4820] CISA, DHS S&T, INL, LSU Help Energy Industry Partners Strengthen Incident Response and OT Cybersecurity, Cybersecurity and Infrastructure Security Agency (Washington D.C.) 23 April 2025. Access Date: 25 April 2025. http://cisa.gov/news-events/news/cisa-dhs-st-inl-lsu-help-energy-industry-partners-strengthen-incident-response-and-ot-cybersecurity

[4821] Statement from Matt Hartman on the CVE Program, Cybersecurity and Infrastructure Agency (Washington D.C.) 23 April 2025. Access Date: 25 April 2025. https://www.cisa.gov/news-events/news/statement-matt-hartman-cve-program

[4822] Ukraine: 3rd Cyber Dialogue with the European Union takes place in Brussels, European Union External Action (Brussels) 15 July 2024. Access Date: 28 October 2024. https://www.eeas.europa.eu/eeas/ukraine-3rd-cyber-dialogue-european-union takes-place-brussels_en national financial stability, reinforcing Lesotho's cybersecurity position within the international community.[4823] This action increases coordination between the EU and Lesotho through the enhancement of attribution processes relating to cybercrime detection and deterrence.

On 4 October 2024, European Union External Action announced that the EU, alongside the North Atlantic Treaty Organization (NATO) participated in a dialogue aimed at reinforcing cooperation between NATO and the EU regarding the detection and deterrence of cybersecurity threats, as well as to increase State coordination of cybersecurity infrastructure.[4824] This improves international collaboration in cyberspace and works to establish a cohesive framework for the deterrence of malicious cyber activities.

On 8 October 2024, the European Council announced that the European Union had adopted a new sanctions framework addressing a multitude of hybrid threats from Russia, including malicious cyber activity, in response to Russia's problematic state behavior abroad.[4825] This action disrupts the infrastructure used by malicious State actors in cyberspace and responds to and deters cybersecurity threats.

On 10 October 2024, the European Council implemented the Cyber Resilience Act, which establishes specific cybersecurity requirements for all products with digital components and/or are connected to a network or device, ensuring their safety prior to market placement and throughout their subsequent lifetime.[4826] This allows consumers to consider cybersecurity when purchasing digital items. This action takes preventative measures against cyberattacks through the disruption of infrastructure and the development of a cohesive legislative framework.

On 29 October 2024, European Commission President Ursula von der Leyen and Prime Minister of Montenegro Milojko Spajić launched the Government Security Operations Center in Podgorica to strengthen Montenegro's cybersecurity measures following a plethora of cyberattacks, in adherence with European Standards.[4827] The project was co-funded by the European Union and operates within the Ministry of Public Administration with a budget of EUR4.4 million. The center establishes a cohesive framework for rapid response and the deterrence of cyberattacks and strengthens collaboration between the European Union and other countries.

On 1 November 2024, High Representative for Foreign Affairs and Security Policy of the European Union and Vice-President of the European Commission Josep Borrell, and the Japanese Minister for Foreign Affairs Takeshi Iwaya participated in a dialogue between the EU and Japan to announce the EU-Japan Security and Defense Partnership which establishes a framework for bilateral cooperation in a variety of security areas, one

[4823] Lesotho - European Union Partnership Launches Cybersecurity Training for Central Bank of Lesotho, Delegation of the European Union to The Kingdom of Lesotho (Maseru) 6 September 2024. Access Date: 28 October 2024. https://www.eeas.europa.eu/delegations/lesotho/lesotho-european-union-partnership-launches-cybersecurity-training-central-bank-lesotho_en

[4824] European Union and NATO hold the first Structured Dialogue on Cyber, European Union External Action (Brussels) 4 October 2024. Access Date: 28 October 2024. https://www.eeas.europa.eu/eeas/european-union-and-nato-hold-first-structured-dialogue-cyber-0_en

[4825] Timeline - EU response to Russia's war of aggression against Ukraine, European Council (Brussels) 8 October 2024. Access Date: 28 October 2024. https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/hybrid-threatsrussia-statement-by-the-high-representative-on-behalf-of-the-eu-on-russia-s-continued-hybrid-activity-against-the-eu-and-its-member-states/

[4826] Cyber resilience act: Council adopts new law on security requirements for digital products, European Council (Brussels) 10 October 2024. Access Date: 28 October 2024. https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/

[4827] European Commission President von der Leyen and Prime Minister Milojko Spajić officially open Cybersecurity Centre, Delegation of the European Union to Montenegro (Podgorica) 29 October 2024. Access Date: 1 November 2024. https://www.eeas.europa.eu/delegations/montenegro/european-commission-president-von-der-leyen-and-prime-minister-milojko-spajić-officially-open_en being cybersecurity.[4828] This agreement deepens international collaboration regarding cybersecurity issues, creating an organized and intentional framework to deter malicious cyber activities.

On 4 November 2024, High Representative Borrell and the Minister for Foreign Affairs of the Republic of Korea, Cho Tae-Yul, held an EU-Korea Strategic Dialogue announcing a defense partnership between both members, aimed at strengthening cooperation on cyber security in the international sphere.[4829] This action unifies state actors and their respective frameworks in cyberspace, allowing for the coordination of attribution processes regarding cyber security.

On 11 November 2024, the European Union External Action announced that the European Union and Japan had held their sixth cyber dialogue wherein both members discussed their legislative developments regarding[4830] Further, they explored possible cooperation on critical infrastructure and cohesive cyber frameworks. This exchange improves international collaboration on cyber security issues, aimed at establishing increased resilience to national and global cyber threats.

On 14 November 2024, the European Union External Action announced that the European Union and Moldova had held a security and defense dialogue in which members shared information on their respective security strategies aimed at deterring global cyber threats.[4831] Both actors underlined the needs to further exchange and strengthen their legislative and infrastructural developments against hybrid threats. This action demonstrates increased international collaboration aimed at developing a cohesive framework to deter malicious cyber activity, as well as to increase transparency between state actors in cyberspace.

On 18 November 2024, the European Council approved the upholding of international legal obligations by state actors in cyberspace.[4832] This action is a response to an increase in global cyber threats and reinforces state compliance to the United Nations framework of responsible state behavior. The EU and its member states have called this the 'Programme of Action' and hope that it will increase global training and capacity building. This action actively responds to malicious state behavior in cyberspace and attempts to develop a cohesive international framework through increased collaboration.

On 19 November 2024, the European Union External Action announced that the European Union and Albania adopted a new security and defense partnership, establishing a framework for cooperation and reinforced resilience in light of increasing global cybersecurity threats.[4833] This partnership increases collaboration between state actors aimed at deterring and responding to malicious state behavior in cyberspace.

[4828] Japan: High Representative/Vice-President holds first EU-Japan Strategic Dialogue with Foreign Minister Takeshi Iwaya, European Union External Action (Brussels) 1 November 2024. Access Date: 1 November 2024. https://www.eeas.europa.eu/eeas/japan-high-representativevice-president-holds-first-eu-japan-strategic-dialogue-foreign-minister_en

[4829] Republic of Korea: High Representative/Vice-President Borrell holds first Strategic Dialogue with Foreign Minister Cho in Seoul, European Union External Action (Brussels) 4 November 2024. Access Date: 1 December 2024. https://www.eeas.europa.eu/eeas/republic-korea-high-representativevice-president-borrell-holds-first-strategic-dialogue-foreign_en

[4830] Cyber: EU and Japan hold 6th Cyber Dialogue in Tokyo, European Union External Action (Brussels) 11 November 2024. Access Date: 1 December 2024. https://www.eeas.europa.eu/eeas/cyber-eu-and-japan-hold-6th-cyber-dialogue-tokyo_en

[4831] Moldova: Security and Defence Dialogue with the EU takes place in Chisinau, European Union External Action (Brussels) 14 November 2024. Access Date: 1 December 2024. https://www.eeas.europa.eu/eeas/moldova-security-and-defence-dialogue-eu-takes-place-chisinau_en

[4832] Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace, European Council (Brussels) 18 November 2024. Access Date: 1 December 2024. https://www.consilium.europa.eu/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/

[4833] Albania: New Security and Defence Partnership with the EU to strengthen capabilities and cooperation, European Union External Action (Brussels) 19 November 2024. Access Date: 1 December 2024. https://www.eeas.europa.eu/eeas/albania-new-security-and-defence-partnership-eu-strengthen-capabilities-and-cooperation_en

On 19 November 2023, the European Union External Action announced that the European Union signed a security and defense partnership with North Macedonia in hopes of establishing[4834] This partnership aims to increase capacities and cooperation in the complex global hybrid environment. This action aims to increase state resilience and cooperation against a variety of cyber threats.

On 3 December 2024, the European Union Agency for Cybersecurity published its biennial report on the state of cybersecurity in the EU.[4835] The report includes six policy recommendations, such as revising the EU Blueprint for cyber incident response, developing the cyber workforce in the EU, and improving supply chain security through enhanced risk assessments and a unified policy framework. It also highlights the increasing importance of Artificial Intelligence and Post-Quantum Cryptography in cybersecurity, with future efforts focused on enhancing operational cooperation and situational awareness to address emerging threats.

On 5 December 2024, the European Union External Action announced that the EU and Norway held a Security and Defence Dialogue and signed the EU-Norway Security and Defence Partnership, aimed at establishing cohesive security measures.[4836] Both actors agreed to hold expert consultations regarding Russia's malicious hybrid and cyber threats.

On 6 December 2024, the European Council approved legislative initiatives for the European Union Agency for Cybersecurity to increase resilience and strengthen responses to cyber security threats, notably through the development of European cybersecurity certification schemes.[4837] This demonstrates the Council's increasing efforts to stabilize infrastructure and policy in the cyber space, taking into consideration the growing scale and complexity of cybercrime.

On 17 December 2024, the European Council imposed restrictive measures against Russia's destabilizing actions abroad not adhering to international law in the cyberspace, directly restricting sixteen individuals and three entities.[4838] These measures demonstrate the member's commitment to counter cybercrime through international measures against actors that fail to uphold principles of international law in the cyberspace.

On 18 December 2024, European Union External Action announced that the EU and Albania had signed the Albania-EU Security and Defence Partnership, affirming their joint efforts to strengthen security and defense in Europe through state cooperation and allowing nations to tackle hybrid threats, misinformation and terrorism.[4839] This act exemplifies the EU's commitment to develop international partnerships on issues of security and defence in order to adequately fight cyber threats through collaborative efforts.

[4834] North Macedonia: New Security and Defence Partnership with the EU to strengthen capabilities and cooperation, European Union External Action (Brussels) 19 November 2024. Access Date: 1 December 2024. https://www.eeas.europa.eu/eeas/north-macedonia-new-security-and-defence-partnership-eu-strengthen-capabilities-and-cooperation_en

[4835] EU's first ever report on the state of cybersecurity in the Union, European Union Agency for Cybersecurity (Brussels), 3 December 2024. Access Date 21 December 2024. https://www.enisa.europa.eu/news/eus-first-ever-report-on-the-state-of-cybersecurity-in-the-union

[4836] Norway: fourth Dialogue on Security and Defence with the EU takes place in Brussels, European Union External Action (Brussels) 5 December 2024. Access Date: 19 February. https://www.eeas.europa.eu/eeas/norway-fourth-dialogue-security-and-defence-eu-takes-place-brussels_en

[4837] ENISA: Council approves conclusions for a stronger EU agency for cybersecurity, European Council (Brussels) 6 December 2024. Access Date: 19 February. https://www.consilium.europa.eu/en/press/press-releases/2024/12/06/enisa-council-approves-conclusions-for-a-stronger-eu-agency-for-cybersecurity/

[4838] Russian hybrid threats: EU agrees first listings in response to destabilising activities against the EU, its member states and partners, Delegation of the European Union to Ukraine (Brussels) 17 December 2024. Access Date: 19 February 2025. https://www.eeas.europa.eu/delegations/ukraine/russian-hybrid-threats-eu-agrees-first-listings-response-destabilising-activities-against-eu-its_en

[4839] Albania: press statement by High representative/Vice-President Kaja Kallas following the Signing of the Security and Defence Partnership, European Union External Action (Brussels) 18 December 2024. Access Date: 19 February 2025. https://www.eeas.europa.eu/eeas/albania-press-statement-high-representativevice-president-kaja-kallas-following-signing-security-and_en

On 18 December 2024, European Union External Action announced that the European Union had held a summit with leaders of the Wester Balkans, wherein all parties adopted the Brussels Declaration which emphasized the significance of countering hybrid threats the manipulation of information via foreign interference, agreeing to increase cybersecurity cooperation and expand strategic communication.[4840] These efforts demonstrate the development of policy and collaboration between member states in order to create increased resilience against threats in the cyberspace.

On 27 January 2025, the European Council enforced restrictive measures against three officers of the General Staff on the Armed Forces of the Russian Federation due to their involvement in malicious cyber activity which took place against the Republic of Estonia in 2020, leading to the theft of confidential government data.[4841] This demonstrates the Council's efforts to counter malicious cyber activity and hold violators of international law accountable for their actions.

On 6 February 2025, the European Commission adopted the fifth annual Work Programme for the European Defence Fund.[4842] Under this programme, the EU allocated EUR40 million of funding towards research and development in cyber security.

On 28 January 2025, the European Parliament's Delegation for Relations with NATO (DNAT) convened to discuss strengthening strategic cooperation in defense and cybersecurity, focusing on enhancing NATO-EU synergies in addressing emerging cyber threats.[4843] The discussions covered collaborative defense measures, including information-sharing frameworks and coordinated responses to cyberattacks. This meeting highlighted the growing importance of joint efforts in building a robust cybersecurity infrastructure that effectively combats transnational cybercrime and malicious digital activities.

On 3 February 2025, President António Costa and other officials discussed the future of EU cybersecurity initiatives emphasizing the need for stronger internal defense mechanisms and international collaboration.[4844] Key points included aligning cybersecurity policies across member states, enhancing digital infrastructure and preparing for evolving cyber threats. This reinforces the EU's commitment to a unified strategy aimed at pre-emptively addressing cybercrime and protecting against cyberattacks that target critical infrastructure.

On 18 February 2025, the DNAT convened to discuss key developments in global cybersecurity policy and NATO's strategic role in defense coordination.[4845] This session reviewed progress on NATO-EU collaboration to improve cyber resilience and enhance collective cybersecurity defense mechanisms. The discussions also included action plans aimed at preventing cybercrime by strengthening intergovernmental cooperation and reinforcing cyber hygiene practices across member states.

[4840] EU-Western Balkans Summit: Building a Future of Peace and Prosperity, European Union External Action (Brussels) 18 December 2024. Access Date: 19 February 2025. https://www.eeas.europa.eu/eeas/eu-western-balkans-summit-building-future-peace-and-prosperity_en

[4841] Cyber-attacks: three individuals added to EU sanctions list for malicious cyber activities against Estonia, European Council (Brussels) 27 January 2025. Access Date: 19 February 2025. https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia

[4842] More than €1 billion from the European Defence Fund to develop next generation defence technologies and innovation, European Commission (Brussels) 29 January 2025. Access Date: 10 March 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_376

[4843] DNAT Meetings, European Parliament (Brussels) 28 January 2025. Access Date: 8 April 2025. https://www.europarl.europa.eu/delegations/en/dnat/home

[4844] Remarks by President António Costa at the Press Conference Following the Informal EU Leaders' Retreat of 3 February 2025, European Union Council (Brussels) 3 February 2025. Access Date: 8 April 2025. https://www.consilium.europa.eu/en/press/press-releases/2025/02/03/remarks-by-president-antonio-costa-at-the-press-conference-following-the-informal-eu-leaders-retreat-of-3-february-2025/

[4845] DNAT Meetings, European Parliament (Brussels) 18 February 2025. Access Date: 8 April 2025. https://www.europarl.europa.eu/delegations/en/dnat/home

On 27 February 2025, the European Parliament and North Macedonia held a meeting focused on bolstering cybersecurity initiatives and regional digital governance frameworks.[4846] Key discussions included enhancing cybersecurity education, promoting regulatory alignment on data protection and establishing joint monitoring mechanisms to detect and respond to cyber threats. This meeting emphasized both regions' commitment to prevent cybercrime by safeguarding their digital ecosystems through synchronized policy development and strategic cooperation.

On 6 March 2025, the European Parliament's Delegation for Relations with the Republic of Korea discussed key cybersecurity challenges and enhanced bilateral cooperation on defense strategies.[4847] This meeting emphasized joint efforts in addressing evolving cyber threats, particularly in the context of state-sponsored cyberattacks and critical infrastructure protection. Through this partnership, the EU and South Korea reaffirmed their commitment to countering cybercrime and reinforcing mutual cybersecurity frameworks for greater resilience.

On 6 March 2025, President Costa addressed key cybersecurity initiatives discussed during the Special European Council meeting, highlighting the importance of EU unity in facing cyber threats.[4848] Officials at the meeting emphasized strengthening cross-border collaboration in digital defense and the need for robust response frameworks to tackle growing cybercrime challenges. This meeting further solidified the EU's resolve to develop proactive policies aimed at deterring and mitigating cybercrime through enhanced defense coordination.

On 6 March 2025, the European Council adopted conclusions to enhance European defense capabilities, with a particular focus on cybersecurity as a core aspect of national security.[4849] The conclusions laid the foundations for deeper collaboration between EU members to address cybersecurity vulnerabilities and counteract the growing threat of cyberattacks targeting EU infrastructure. These measures aim to prevent cybercrime by strengthening the EU's collective defense against malicious digital activities and securing critical assets.

On 20 March 2025, the DNAT discussed the evolving threat landscape of cybersecurity and the necessity for enhanced NATO-EU collaboration.[4850] This meeting underscored the need for shared intelligence, joint military-cyber defense capabilities and strategic planning to address increasing cyber threats. The session emphasized cooperative efforts to prevent cybercrime by fostering a more unified defense approach to digital vulnerabilities and malicious state-driven cyber activities.

On 27 March 2025, the EU and various Central Asian countries issued a joint communiqué following the 20th EU-Central Asia Ministerial Meeting, highlighting strengthened cybersecurity cooperation.[4851] The communiqué detailed initiatives to enhance digital resilience, with a focus on combating cybercrime, securing critical infrastructure and building cybersecurity capacity in the region. This collaboration aims to prevent the

[4846] Inter-Parliamentary Meetings, European Parliament (Brussels) 27 February 2025. Access Date: 8 April 2025. https://www.europarl.europa.eu/delegations/en/d-mk/activities/inter-parliamentary

[4847] DKOR Ordinary Meeting, European Parliament (Brussels) 6 March 2025. Access Date: 8 April 2025. https://www.europarl.europa.eu/delegations/en/dkor-ordinary-meeting-thursday-6-march-2/product-details/20250304DPU39855

[4848] Remarks by President António Costa at the Press Conference Following the Special European Council Meeting of March 6 2025, European Union Council (Brussels) 6 March 2025. Access Date: 8 April 2025. https://www.consilium.europa.eu/en/press/press-releases/2025/03/06/remarks-by-president-antonio-costa-at-the-press-conference-following-the-special-european-council-meeting-of-6-march-2025/

[4849] European Council Conclusions on European Defence, European Union Council (Brussels) 6 March 2025. Access Date: 8 April 2025. https://www.consilium.europa.eu/en/press/press-releases/2025/03/06/european-council-conclusions-on-european-defence/

[4850] DNAT Meetings, European Parliament (Brussels) 20 March 2025. Access Date: 8 April 2025. https://www.europarl.europa.eu/delegations/en/dnat/home

[4851] Joint Communiqué Following the 20th EU-Central Asia Ministerial Meeting, European Union Council (Brussels) 27 March 2025. Access Date: 8 April 2025. https://www.consilium.europa.eu/en/press/press-releases/2025/03/27/joint-communique-20th-eu-central-asia-ministerial-meeting/

exploitation of cyber vulnerabilities by criminal actors and ensure collective defense against emerging cyber threats.

On 27 March 2025, the European Commission approved the 2025–2027 agenda for the Digital Europe Programme, allocating EUR1.3 billion to advance critical digital initiatives across the EU.[4852] The funding will support areas such as artificial intelligence, cybersecurity and workforce development, with a focus on boosting Europe's technological independence. Key efforts include deploying cyber defense tools, enhancing digital infrastructure and safeguarding essential services like healthcare facilities and undersea communication networks.

On 11 April 2025, the European Commission opened a public consultation to assess and update the 2019 EU Cybersecurity Act.[4853] The review aims to bolster the EU's cyber resilience by re-evaluating the mandate of the European Union Agency for Cybersecurity, enhancing the cybersecurity certification system and tackling security risks in ICT supply chains. It also seeks to streamline existing regulations and reporting processes to make compliance easier for businesses while reinforcing protection standards.

On 15 April 2025, the European Commission announced EUR140 million in new funding opportunities through the Digital Europe Programme to accelerate the adoption of key digital technologies.[4854] The initiative focuses on integrating generative AI in public services, expanding digital skills training and establishing a European fact-checking network to combat disinformation. Additional funding will support the growth of Digital Innovation Hubs and enhance online safety infrastructure, advancing the EU's efforts to build digital resilience and strengthen cybersecurity across Member States.

The European Union has fully complied with its commitment to developing and using tools to deter and respond to malicious (State) behavior and to cyber criminals, and disrupt the infrastructure they use, including by enhancing coordination on attribution processes. The EU has taken strong action towards the development of systems and technology directly aimed at preventing and reacting to cyber threats through the establishment of organized infrastructure and regulatory frameworks. Furthermore, the EU has taken both strong and weak actions towards h the improvement of international collaboration on cybersecurity frameworks and cyberattack identification via co-operative dialogues addressing threats, and the implementation of sanctions regimes and cybersecurity programs abroad. Thus, the EU has taken strong action to develop tools, prevent cybercrime, respond to cybercrime, disrupt criminal infrastructure, and enhance coordination on the attribution process.

Thus, the European Union receives a score of +1.

Analyst: Marta Tavares Fernandes

[4852] Commission to invest €1.3 billion in artificial intelligence, cybersecurity and digital skills, European Union Council (Brussels) 27 March 2025. Access Date: 25 April 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_907

[4853] Commission opens consultation on revising EU Cybersecurity Act, European Commission (Brussels) 11 April 2025. Access Date: 25 April 2025. https://digital-strategy.ec.europa.eu/en/news/commission-opens-consultation-revising-eu-cybersecurity-act

[4854] Commission invests €140 million to deploy key digital technologies, European Commission (Brussels) 15 April 2025. Access Date 25 April 2025. https://digital-strategy.ec.europa.eu/en/news/commission-invests-eu140-million-deploy-key-digital-technologies