Cybersecurity Coalition

EU POLICY ROADMAP

2024 - 2029

MISSION STATEMENT

The war in Ukraine has demonstrated the fundamental role the digital domain will play in future international conflicts, and how widely the impacts of malicious cyber actors can be felt across different industries, sectors, and borders. Destructive cyber-attacks, often combined with kinetic strikes, by Russian government-backed actors targeted far more than just Ukrainian government and military entities, expanding their scope to include critical infrastructure, utilities and public services, and the media and information space too. These attacks have highlighted the need to address cybersecurity risk and bolster the resilience of critical infrastructure around the world.

The power of international cooperation and partnership to support collective defence and more resilient cybersecurity has been a significant factor in ensuring Ukraine has been able to continue to provide essential services to its citizens. Almost immediately, industry and governments around the world mobilized to provide cybersecurity assistance to Ukraine. Recently, European Union (EU) support was formalized via a cyber cooperation agreement in November 2023 between the European Union Agency for Cybersecurity (ENISA) and Ukraine's National Cybersecurity Coordination Centre (NCCC).

The war shows how enhanced and wider international cooperation can enable a more robust and resilient global cybersecurity ecosystem, while ensuring the sovereignty of nation under attack. As the largest trading bloc globally, the EU has established a foundation of cybersecurity policy and certifications – some voluntary, some binding. The EU's legislative focus has only expanded to address emerging technologies like artificial intelligence and quantum computing.

The passage of the Cyber Resilience Act (CRA) and the AI Act, as well as the upcoming elections, offer the EU an opportunity to establish a new vision for collective digital resilience. As the EU is confronted with new cybersecurity and technology risks maintaining focus on working toward a more secure and resilient European cyber landscape is paramount. Creating greater digital resilience requires those tasked with advancing the EU's future safety and prosperity to implement necessary policies without siloing Europe from the global cyber ecosystem.

A roadmap to ensure Europe's collective digital resilience in the years ahead should seek to incorporate the following factors:

1. STRENGTHEN THE EUROPEAN CYBERSECURITY ECOSYSTEM

The EU should take policy steps to ensure its digital workforce and industry partnership model is able to respond to a major cyber incident, potentially in a time of conflict. In this effort, a stronger and more robust relationship with trusted industry partners will be vital, including greater information sharing. Europe must also continue to take steps to strengthen the cybersecurity workforce and best practice adoption across member states.

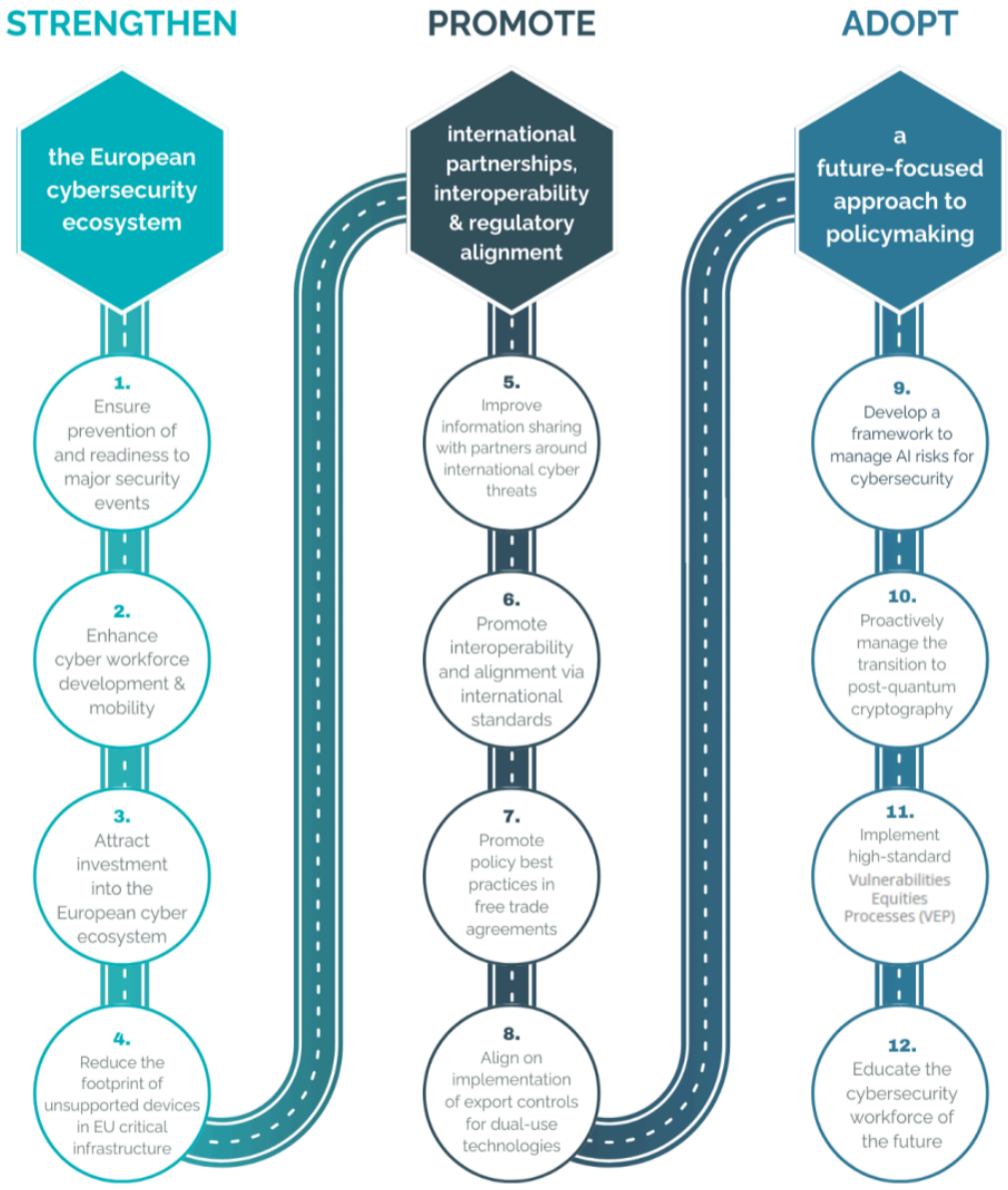
2. PROMOTE INTERNATIONAL PARTNERSHIPS, INTEROPERABILITY & REGULATORY ALIGNMENT

Interoperability with non-EU partners is increasingly vital for cyber resilience, as the war in Ukraine made abundantly clear. Many international partners stand ready and willing to engage in cooperation through information sharing, free trade agreements, and more. Europe should seek to engage proactively across the Atlantic, through the G7, and with emerging international groupings like the Quadrilateral Security Dialogue (Quad). Aligning cybersecurity regulation between the EU and the US, as well as other key jurisdictions, is imperative. Alignment around regulatory best practices and lessons learned will enhance collective cyber resilience, while enabling industry to focus on operational security investments, rather than an unnecessarily complex global system of compliance regimes.

3. ADOPT A FUTURE-FOCUSED APPROACH TO POLICY MAKING

Lastly, Europe needs to set itself up for long term success by future-proofing its cybersecurity environment. At the forefront of this is ensuring that cybersecurity and risk management are proactively incorporated into dialogue around emerging technologies such as artificial intelligence and quantum computing. Europe must also lay the groundwork for a sustainable and skilled cyber workforce to lead in these areas.

2024-2029
EU POLICY ROADMAP



STRENGTHEN THE EUROPEAN CYBERSECURITY ECOSYSTEM

1. Ensure prevention of and readiness to respond to major security events.

The Cyber Solidarity Act (CSA) will help assist in creating a robust framework for responding to such major cyber incidents. Finalization of the CSA will ensure the EU and its member states benefit from a more robust and institutionalized relationship with industry, leveraging their cutting-edge capabilities.

Building on aggregate information sharing requirements already laid out in the CRA and the Network and Information Security Directive (NIS 2), the EU is well placed to create a better framework for information sharing which will prepare critical infrastructure to respond to major attacks. Bi-directional information sharing where governments aggregate private sector reporting, coupled with the unique insights governments can generate will allow for remediation of vulnerabilities before threat actors can exploit them.

The Australian government, for example, is implementing a robust two-way information sharing mechanism in which industry data is aggregated, supplemented with government intelligence, and shared across national critical infrastructure. It may also allow the government to draw on expertise in industry to detect trends in cybersecurity incidents and engage in more targeted mitigation strategies or pre-emptively bolster cyber defences against a certain threat actor or type of cyber incident.

Additionally, the EU could scope the feasibility of a more comprehensive early warning system for cyber incidents. The UK has an early warning program that uses reports from security researchers to alert impacted organizations.[1] An early warning system and other government information sharing should not necessitate additional incident reporting requirements, instead the government should internally triage information gathered through requirements established in the CRA to serve both the government and industry.

Recommendations

- Finalize the Cyber Solidarity Act to institutionalize a more robust partnership with industry to both prevent and address major security incidents.
- Implement more robust threat information sharing mechanisms that ensure a two-way exchange of information.

[1] Early Warning, UK National Cyber Security Centre (May 2021)

2. Enhance cyber workforce development and workforce mobility.

The EU is facing a cybersecurity workforce shortage. Building on initiatives like the Cybersecurity Skills Academy and Cybersecurity Skills Framework, while partnering with academia and industry to identify workforce needs, will be important in ensuring a more secure Europe.

The Cybersecurity Skills Framework provides a comprehensive baseline rubric for cybersecurity roles and associated skills. Against a backdrop of rapid deployment of artificial intelligence and quantum computing grows, relevant educational resources and standards will also need to be created, as well as workforce pipelines. These should emphasize the intersection of these and other emerging critical technologies with cybersecurity to ensure a comprehensive approach to European cybersecurity.

The EU should also leverage relationships with private organizations and institutions to develop dedicated pathways for people to enter the workforce. EU institutions should seek to build stronger relationships with industry to create apprenticeship and internship program through incentives for collaboration and promoting best practices. Encouraging the development of hands-on learning experiences for students, such as cybersecurity clinics through funding or other resources will also ease the transition to the workforce by allowing students to develop more work ready skills.

Tapping into the potential employees outside of the industry who are mid-career to upskill or reskill will offset the talent pipeline. Taking concrete steps to diversify the cybersecurity workforce, such as by providing greater access to education and credentialing, will also help to diversify the ideas and innovation to tackle complex cyber issues. Many national cyber strategies include provisions for growing the cyber workforce, such as Australia[2] and Singapore[3], while some countries have dedicated cyber workforce strategies (such as the United States).[4] . EU is well positioned to learn from international partners and create a best practice workforce development model/

Recommendations

- Work with academia and industry to continue developing hands-on learning experiences for students, including apprenticeships, internships, and cybersecurity clinics.
- Increase accessibility to education and credentialing for mid-career employees and civil servants.
- Work with international partners to create a common baseline for cyber skills.

[2] 2023-2030 Australian Cyber Security Strategy, Australian Department of Home Affairs (November 2023)
[3] Singapore Cybersecurity Strategy 2021, Cyber Security Agency of Singapore (October 2021)
[4] U.S. National Cyber Workforce and Education Strategy, U.S. Office of the National Cyber Director, Executive Office of the President (July 2023)

3. Attract investment into the European cyber ecosystem.

Inbound investment in digital services and technology is fundamental to the future prosperity of the EU. In order to ensure this, financial measures, such as incentives for research and development, procurement policy, and innovation pilots, as well as also non-financial incentives are required. Incentives should be non-discriminatory – available to both EU and non-EU headquartered companies – if the associated investments take place in Europe.

To continue growing European competitiveness in the technology sector, Europe must continue to expand programs to provide tools, resources, and opportunities to start-ups and small- and mid-sized enterprises. Inspiration can be drawn from partner countries that have established various programs. For example, Australia is establishing a Cyber Security Challenge program to promote innovation and support growing enterprises in the cybersecurity sector. The U.S. has recently launched the National AI Research Resource (NAIRR) pilot, which will provide researchers and educators with access to resources needed for advanced AI research.[5] Investments in these areas will drive economic growth in Europe. It is also vital that the government works with industry to ensure that research and development is targeted to solve real-world problems and can be translated to products and solutions for the market.

Non-financial measures can also help stimulate investment in the EU, with harmonization of respective regulatory regimes enabling seamless investment.

Recommendations

- Establish incentives for research and development, procurement policy, innovation pilots, etc.
- Implement non-financial incentives such as ensuring interoperability of regulatory requirements both within the EU and internationally.
- Ensure that incentives are available to both EU and non-EU headquartered companies.
- Bolster investment in enterprise open-source technology and open standards to ensure resilience and optimise interoperability of solutions and cyber threat knowledge.

[5] NAIRR Pilot, U.S. National Science Foundation (January 2024)

4. Reduce the footprint of unsupported devices in EU critical infrastructure.

Critical infrastructure relies on a vast array of computing technologies, both hardware and software, which must be managed and maintained as a collective stack. Disruptions to any single component can catastrophically cascade to other components, other critical infrastructure providers, and to the global technology ecosystem at large. To ensure these components are as safe, reliable, and resilient as possible, technology vendors provide support for their products for a designated lifetime – but increasing resource costs mean they cannot be supported indefinitely. As the technology and threat landscapes evolve, updates to older products can become increasingly expensive to produce and deploy. The issue is exasperated by the often-bespoke nature of critical infrastructure technologies, which may also be deployed in remote or otherwise non-traditional locations and scenarios.

Despite these challenges slowing or preventing the updating and upgrading of devices and software, it remains crucial to reduce the overall footprint of these components. End-of-life/end-of-support products enhance the attack surface for threat actors, as weaknesses found in unsupported products will remain unpatched and easy to exploit. While exceptions should be made in certain circumstances (e.g., post-merger integration, impacts to networks with little tolerance for downtime) the default should be the removal of all unsupported devices from networks, with extensions granted on a case-by-case basis. Such an approach has already been taken in countries such as Japan.[6]

When removal of out-of-date products is not possible or deemed infeasible, mitigating controls and best practices should be used to closely protect these vulnerable devices. These protections should be a step above what is otherwise required by law or best-practice.

The impact of unsupported and unpatched devices cannot be overstated and must be reduced to protect critical infrastructure from potentially devastating cyber-attacks. The responsibility of tackling this challenge falls on both the technology operators and vendors.

Recommendations:

- Align procurement requirements with well-known security best practices and standards and request clear end-of-life information in contracts.
- Increase cybersecurity diligence (e.g., vulnerability scanning, configuration management, mitigating controls, and in the context of open source, bolstering the use of backporting and rebasing) on products that are outside of their support period.
- Periodically ensure that product configuration is aligned with vendor recommendations, with increasing frequency as products age

[6] Article 52.1, Economic Security Promotion Act, Cabinet Office of the Government of Japan (May 2022)

PROMOTE INTERNATIONAL PARTNERSHIPS, INTEROPERABILITY & REGULATORY ALIGNMENT

5. Improve information sharing with partners on international cyber threats.

A legislative foundation for substantive public-private sector threat information sharing in the EU was laid by regulations and directives like GDPR, NIS 1 and 2, and the EU Cybersecurity Act. International collaboration on threat information sharing should come hand in hand with this, allowing Europe to leverage the resources and knowledge of partner governments more effectively. Threat information can include indicators of compromise, as well as the tactics, techniques and procedures (TPPS) used by threat actors.

One key aspect of this is better aligning cybersecurity regulation, namely incident reporting and vulnerability reporting requirements. When definitions and timelines vary, it complicates the ability to compare cyber threat actors' behaviour, impact, and methods. Considering that some cybersecurity regulation remains nascent, mechanisms to coordinate internationally among regulators also remain nascent.

Cybersecurity threats are inherently international, and a collective and collaborative approach will increase the EU's ability to defend against increasingly sophisticated adversaries and better track emerging threats. In December 2023, the European Union Agency for Cybersecurity (ENISA) and the US Cybersecurity and Infrastructure Security Agency (CISA) formalized a broad information sharing agreement to tackle growing security threats. This effort should serve as a model to be replicated by ENISA with other partner nations.

To ensure that the benefits of this are realized by both public and private-owned entities, the EU and its partners should explore how best to ensure that information is proactively shared with industry to reduce the frequency and magnitude of incidents.

Recommendations:

- Engage with international partners to identify threat information sharing opportunities.
- Establish formal exchanges for threat information sharing with international partners, leveraging existing mechanisms, such as the International Counter Ransomware Initiative, the CVE® Program, FIRST, Interpol, etc.

6. Promote interoperability and alignment via international standards and regulatory cooperation.

Ensuring international interoperability of cybersecurity requirements – whether through mutual recognition agreements or the use of international standards – is also important in ensuring that the cybersecurity industry has fewer variables to navigate while providing necessary services. Officials are already engaging in work on a mutual recognition agreement between the Cyber Resilience Act in the EU and the Cyber Trust Mark in the U.S. to ensure that manufacturers can focus on their products and not the steps necessary for individual validation processes.

It will be useful to identify and engage with partners and allies who are already engaged in other areas covered by the Cyber Resilience Act and the cybersecurity certification framework, such as Software Bill of Materials (SBOM), secure software development, or cloud security. Mutual recognition agreements in these areas can ease burdens on organizations and may allow international organizations to operate within Europe and European countries to operate internationally with more ease. Some member states have already engaged in mutual recognition arrangements; for example, the German Federal Office for Information Security (BSI) signed a mutual recognition agreement with Singapore on the German IT Security Label and Singapore's Cybersecurity Label.[7] Capitalizing on the existing desire of member states to engage with international patterns can help Europe further grow its competitiveness in the technology and cybersecurity sectors.

Increased regulatory cooperation and alignment on incident reporting, such as a common form and a common understanding of the timeline for incident reporting, would have a beneficial impact on companies and organizations operating across multiple jurisdictions. Working with allies such as NATO, where there is existing political will to engage with the EU on cybersecurity, to develop more streamlined incident reporting processes will likely reduce burdens on organization and allow them to report necessary information more accurately.

Lastly, as other countries set security standards, particularly for emerging technologies, it will be to work proactively to avoid regulatory divergence. By engaging on these standards early, the EU can develop complementary standards with partners and help set international standards ex ante, rather than the more challenging task of ensuring interoperability ex post.

Recommendations

- Where applicable, engage with international partners to develop mutual recognition agreements for certifications or product labels.
- Develop common taxonomies and reporting mechanisms for incident, vulnerabilities, and threat information sharing.
- Engage early with partners to ensure the interoperability of approaches to emerging tech.

[7] BSI and Singapore Cyber Security Agency Mutually Recognise Cyber Security Labels, German Federal Office of Information Security (October 2022)

7. Promote policy best practices through free trade agreements (FTAs).

Digital trade is a vital part of the global economy, and cybersecurity is fundamental to ensuring the integrity and delivery of digital products and services. Free Trade Agreements (FTAs) have the potential to drive the consistent adoption of cyber policy best practices across multilateral groups, while proactively avoiding unnecessary non-tariff barriers to trade.

Since the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) first incorporated cybersecurity provisions into a trade agreement, dozens of countries have now followed suit, including almost all of the world's largest economies. In recent years, FTAs have incorporated commitments on cyber capacity building, operational collaboration/incident response, cyber workforce development, use of risk-based approaches, and the use of international standards in cyber policymaking. In perhaps the most ambitious FTA cyber provision to-date, the UK-Singapore Digital Economy Agreement includes an agreement to implement a mutual recognition agreement on cyber labelling.

The EU has ratified numerous trade agreements with a dedicated digital trade chapter, albeit only one with explicit cybersecurity language: the EU-New Zealand FTA. In this agreement, language only goes as far as establishing a link between cybersecurity and digital trade.

Negotiations of future agreements, whether bilateral or plurilateral, like that of the WTO JSI on eCommerce, should be seen as opportunities to overcome fragmentation and set international best practices by incorporating ambitious cybersecurity language that enhances cybersecurity outcomes while avoiding unnecessary non-tariff barriers to trade.

Recommendations:

In future trade agreements, the EU should incorporate a digital chapter with ambitious cybersecurity language, including:

- Commitments to provide mutual support in responding to cybersecurity incidents;
- A commitment to the use of risk management-based approaches to cybersecurity policymaking;
- A commitment to the use of consensus-based international standards in cybersecurity policymaking;
- The promotion of a common approach to coordinated vulnerability disclosure, grounded in international standards; and
- Mutual recognition agreements, common regulatory baselines and other means to remove unnecessary non-tariff barriers to trade.

8. Align on the implementation of export controls for dual-use cybersecurity technologies.

Malicious actors are taking advantage of the deteriorating geo-political landscape coupled with the evolution of existing cybersecurity capabilities and the development of new capabilities to penetrate networks. Restricting their access to these capabilities, like spyware, must be an international effort.

This can be achieved through renewed efforts in existing multilateral export regimes such as the Wassenaar Arrangement, as well as more recent efforts such as the Pall Mall Process.

The consensus-based nature of export regimes like Wassenaar has led inadequate action to address new threats. While the EU is not a member of these regimes, its member states are. More robust coordination between the EU, its member states, and other likeminded government, can help influence the other members of the regime to set new controls.

While the EU currently lacks the flexibility of other governments such as the U.S. to impose unilateral export control standards,[8] the renewed focus on the issue within the 2023 European Economic Security Strategy highlights the potential for more effective EU coordination of export controls through policy reform.

Recommendations

- Consult and engage with individual member states to better harmonize export control obligations.
- Create a senior-level forum for political coordination on export controls across all member states.
- Utilize the EU-U.S. Trade and Technology Council to coordinate export controls.

[8] The EU does not issue export licenses itself, but rather, establishes dual-use export control regulations for its member countries.

ADOPT A FUTURE-FOCUSED APPROACH TO POLICYMAKING

9. Develop a framework to manage Artificial Intelligence (AI) risks to cybersecurity.

AI will be a tool and a target for attackers and defenders in cyberspace. Malicious actors will use AI tools to enhance and upscale their attacks, employing generative AI in tailored disinformation campaigns and other models to identify network vulnerabilities.

Without stifling innovation, regulators must promote responsible applications of AI, protect the integrity and functionality of security-related AI models as part of ensuring robust and proactive cybersecurity protections, and work with industry to mitigate malicious applications of AI.

The EU is already exploring the intersection between AI and cybersecurity. The AI Act mandates that a high-risk AI system "achieve an appropriate level of accuracy, robustness, and cybersecurity" throughout its lifecycle. Similarly, the European Union Agency for Cybersecurity's (ENISA) recent report on Artificial Intelligence and Cybersecurity Research[9] highlights the importance of securing AI systems and using AI to defend cyberspace. In the report, ENISA recommends creating: 1) test beds to optimize ML-based cybersecurity tools; 2) AI-based penetration testing tools; 3) standardized frameworks to assess the privacy and confidentiality of information flows; 4) AI training for practitioners; and 5) an observatory for AI and cybersecurity threats - all of which are important elements to enable cybersecurity tools that are responsive to the most advanced, AI-enable cyber threats.

Recommendations

- To build AI-enabled cybersecurity tools, developers require comprehensive and representative datasets. EU regulators must guarantee developers' access to these datasets, including cybersecurity datasets of European origin.
- Researchers must have adequate access to resources to create AI-enabled cybersecurity tools. The EU should earmark funding for research and development at the intersection of AI and cybersecurity.
- Existing cybersecurity frameworks and testing bodies are sufficient to evaluate AI-enabled cybersecurity tools. ENISA should take charge on evaluation and testing, seeking coordination with the new EU AI Office where appropriate.
- The EU should seek to educate policymakers and practitioners about the role of AI in the cybersecurity ecosystem. Moreover, as the EU develops AI workforce initiatives, it should foster the growth of the intersectional AI-cybersecurity sector.
- ENISA should develop a dedicated AI cybersecurity framework This would highlight best practices for organizations seeking to use AI to enhance their cybersecurity capabilities and protect their AI systems from cyber threats.

[9] Artificial Intelligence and Cybersecurity Research, European Union Agency for Cybersecurity (June 2023)

10. Proactively manage the transition to post-quantum cryptography.

Post-Quantum Cryptography (PQC) has the potential to upend cryptography, impacting cybersecurity capabilities. The biggest risk is that the data that is encrypted today may not be encrypted in the future. It will be important to anticipate the needs of the industry and set standards for post-quantum technology, while also allowing flexibility as more becomes known and new risks emerge. This will allow the EU to harness the benefits that quantum computing may have on cybersecurity and prevent potential risks. Several countries have already begun work in this domain. The National Institute of Standards and Technology (NIST)[10] is in the process of developing standards for quantum-safe technology, and the National Cyber Security Centre[11] will follow the outcome of this process with recommendations for specific algorithms for representative use cases. Preparing for a post-quantum world also features in the Australia[12] national cybersecurity strategy, with a particular focus on ensuring that guidance is in place for prioritizing and securing critical and sensitive data.

Awareness of quantum and development of workforce and education pathways is also required. Increasing awareness now will set Europe up for success as quantum computing becomes more available and in transitioning to PQC. awareness must highlight to government institutions and organizations across Europe the importance of developing and transitioning to PQC.

Focus should then be given to transitioning government institutions, Member States, critical infrastructure, and organizations to PQC. This is vital in ensuring the security of critical information and systems. The EU will need to gather experts from across industry and academia to develop standards and best practices to ensure consistent adoption across all Member States. Standards and best practices will also be necessary to maintain security during PQC migration. Investments also need to be ramped up to accelerate the vital transition to PCQ.

Continuing to include industry in initiatives like the European Quantum Communication Infrastructure (EuroQCI) is also vital in commercializing new technologies and innovations. This will further propel European technology and industrial capabilities and increase the competitiveness of Europe's technology market.

Lastly, Europe should also pursue avenues for international cooperation, both in innovation and research and in setting standards. Working with other entities that are already developing standards and PQC practices, such as NIST, will accelerate the EU's work.

Recommendations

- Secure the transition to PQC by developing a clear roadmap for the transition of critical infrastructure, including clear and transparent expectations of timelines.
- Ensure that European requirements for PQC protocols are grounded in international standards and best practices.
- Ensure industry involvement to capitalize on new innovations and build the European technology ecosystem.

[10] Post-Quantum Cryptography Standardization, National Institute of Standards and Technology, U.S. Department of Commerce (November 2023)
[11] Preparing for Quantum-Safe Cryptography, UK National Cyber Security Centre (November 2020)
[12] 2023-2030 Australian Cyber Security Strategy, Australian Department of Home Affairs (November 2023)

11. Implement high-standard Vulnerabilities Equities Processes (VEP).

When EU member state governments learn about computer security vulnerabilities, the government may choose to retain the vulnerability for 'offensive' purposes or choose to disclose the vulnerability to the affected vendors so that it can be patched. Timely disclosure of vulnerabilities to affected vendors enables them to mitigate the vulnerabilities, enhancing the security of the technology ecosystem and protecting people before malicious actors can use the vulnerabilities to cause harm. However, vulnerabilities may also be used by governments for law enforcement investigations, intelligence collection, or other 'offensive' purposes to protect national security.[13] The process for considering whether to disclose or retain vulnerabilities may be called a 'government disclosure decision process' (GDDP), 'government vulnerability disclosure' (GVD), or 'vulnerabilities equities process' (VEP).[14]

The Cybersecurity Coalition encourages member states establish such processes. GDDPs prioritize the public's interest in cybersecurity, help protect core Internet infrastructure, provide a key measure of oversight of government hacking activities, and strengthen trust in the security of information technology systems – while also providing governments with the flexibility to preserve necessary 'offensive' cyber capabilities. Declining to adopt GDDPs would set an international precedent that undermines transparency, trust, and security. At present, very few EU member states have publicly announced that they have implemented or are implementing such processes.

The upcoming implementation of the Cyber Resilience Act (CRA) heightens the urgency of establishing processes for governments to responsibly disclose the vulnerabilities they encounter. The CRA requires global manufacturers of software and connected products to swiftly disclose exploited vulnerabilities to multiple government agencies, even if the vulnerabilities are not mitigated.[15] The CRA does not place any restriction on how governments may use vulnerabilities that are shared mandatorily or voluntarily, which has raised concerns among global technology experts and civil society groups in Europe that member state governments will use disclosed vulnerabilities for 'offensive' purposes.[16] Establishing transparent, balanced GDDPs is needed to help ensure that trust in sharing under the CRA will not be undermined by the operational activities of any individual member states.

[13] The Future of Vulnerabilities Equities Processes Around the World, Sven Herpig & Ari Schwartz, Lawfare (January 2019)
[14] Software Vulnerability Disclosure in Europe pg. 63, Centre for European Policy Studies (June 2018)
See also, The Equities Process, U.K. National Cyber Security Centre (November 2018)
[15] Cyber Resilience Act Article 11, Council of the European Union (December 2023)
See also, Preparing for the EU Cyber Resilience Act, Venable LLP (January 2024)
[16] *See, e.g.*, Joint Letter of Experts on CRA's Vulnerability Disclosure Requirements (October 2023)
See also, Joint Statement Raising Concerns on Unpatched Vulnerability Reporting in the CRA (June 2023)

Elements of a government vulnerability disclosure decision process

A GDDP does not obligate a government to disclose vulnerabilities in all circumstances, nor does it implicate how a government acquires or exploits vulnerabilities. Instead, a GDDP establishes a formal decision-making process for a national government to consider whether and how to disclose a vulnerability to affected organizations or to delay disclosure. Some of the basic components of the process include:

1) **Scope.**
The process should encompass computer security vulnerabilities that are purchased, developed, or otherwise acquired by all government organisations and personnel.

2) **Threshold for consideration.**
A vulnerability should be submitted to the process if the vulnerability is not publicly known. This includes new or "zero-day" vulnerabilities, as well as vulnerabilities that the vendor is not aware of or that have not been otherwise made public.

3) **Participants.**
Government agencies that participate in the process should include not just law enforcement and intelligence agencies, but also agencies tasked with defending the security of consumers, businesses, and critical infrastructure.

4) **Equities to consider.**
There should be a strong presumption of disclosure of a vulnerability to the affected organization in order to protect civil liberties, public safety, trade, and IT security. If a government wants to withhold disclosure of a vulnerability, there should be a critical need to do so that outweighs the other considerations.

5) **Temporary retention.**
If a government retains a vulnerability, the retention should only last as long as the critical need outweighs the benefits of disclosure. Retained vulnerabilities must be kept secure. The decision to retain vulnerabilities should be periodically revisited.

6) **Disclosure.**
When a government discloses a vulnerability to an affected organization, it should prioritize disclosure to the owner or maintainer of the vulnerable software or system for the purpose of mitigation.

7) **Transparency and oversight**.
The process should be subject to independent oversight and periodic public reporting. The existence of the process must be made public to engender trust.

Recommendations

- Develop a GDDP toolkit for member states to better understand the topic and associated best practices.
- Work with member states to develop and implement a GDDP at the national level.
- ENISA should be available to support member states, as needed, as they implement GDDP programs.
- Member states that establish a GDDP should consider drawing on the experiences of Germany, the Netherlands, the United Kingdom, the United States, and other nations with similar processes.[17]

[17] Centre for European Policy Studies, Software Vulnerability Disclosure in Europe, June 2018, pg. 64, https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges.

12. Educate the cybersecurity workforce of the future.

Developing cyber skills during early education is vital for long-term prosperity and workforce development. By encouraging schools to teach technology and cybersecurity skills at an early stage of education, the EU can improve the general cybersecurity of citizens and encourage more students to study cybersecurity. There is already a major push in national cybersecurity and workforce strategies to improve digital literacy, foundational skills, and awareness of cyber careers , such as in strategies put out by Australia[18] and the U.S.[19]

Basic cyber hygiene should be encouraged from an early age, such as basic password management, to build skills that can be transferred to personal and work lives, even for those who do not enter a cybersecurity or technology field. This is particularly vital as technology becomes more prevalent for primary education and may help build a foundation for a more cyber secure Europe in the long term. The government can support such efforts by working with education and academic institutions to develop resources and guidelines for appropriate lessons across different education levels.

Additionally, resources and guidelines should be developed for building digital literacy and foundational skills early and should be coupled with increased awareness of technology and cybersecurity careers and interdisciplinary studies. In addition to resources, the government should also consider establishing free programs or courses for young adults interested in exploring cybersecurity topics. The UK has launched a CyberFirst program[20], which provides free courses and competitions for 11-17 year olds, with various hubs targeting different skills and demographics. These efforts are important in maintaining and growing the cybersecurity workforce pipeline. It will also be vital for continued innovation and economic prosperity in Europe and for Europe to take increased advantage of opportunities derived from artificial intelligence, quantum computing, and other emerging technologies.

Recommendations

- Develop resources and guidelines for schools and young adults to encourage early interest in technology and cybersecuri

[18] 2023-2030 Australian Cyber Security Strategy, Australian Department of Home Affairs (November 2023)
[19] U.S. National Cyber Workforce and Education Strategy, U.S. Office of the National Cyber Director, Executive Office of the President (July 2023)
[20] CyberFirst, U.K. National Cyber Security Centre (May 2016)

Cybersecurity Coalition

ABOUT THE CYBERSECURITY COALITION

Companies with security products and services have a unique and important point of view to share with legislators and policymakers. To offer the expertise of the cybersecurity technology industry on critical policy issues - ranging from the role of privacy in security processes to the development of roles and responsibilities for vulnerability researchers to the establishment of security standards for the U.S. government's $14 billion (and growing) annual cybersecurity projects - several leading companies founded the Cybersecurity Coalition.

To achieve its mission, the Coalition monitors and addresses interactions and intersections between government entities, researchers, and vendors. The Coalition promotes its mission in Congress, federal agencies, international standards bodies, industry self-regulatory programs, and relevant policymaking venues.

Guided by its mission and focused on achieving near-term goals and long-term improvements in the cybersecurity space, the Coalition is focused on several active and critical policy issues that require close alignment and coordination to protect the vital interests of the cybersecurity products industry, including:

- Promoting responsible vulnerability research and disclosure;
- Promoting effective privacy processes within cybersecurity policy;
- Establishing government requirements for agency systems;
- Increasing information sharing and threat intelligence; and
- Promoting sound cybersecurity practices in government at all levels.

To educate policymakers with respect to these and related issues, the Coalition engages in the full range of advocacy measures on behalf of the industry, including submitting written comments, offering testimony at congressional and regulatory hearings, drafting legal and policy white papers, engaging with policymakers directly, and holding events.

General Inquiries
info@cybersecuritycoalition.org

Press Inquiries:
pr@cybersecuritycoalition.org
202-667-4967