Istituto Affari Internazionali

ISSN 2532-6570

IAI COMMENTARIES 24 | 22 - MAY 2024

Technological Innovation and Cybersecurity: The Role of the G7

by Ettore Greco and Federica Marconi

In an era of unprecedented technological advancement, digital transformation is revealing its enormous potential, but also presenting new challenges. At its core, it represents a catalyst for innovation, igniting advancements that enhance productivity and propel economic growth. Thus, harnessing its transformative power holds the promise of unlocking new opportunities, solving complex challenges and ultimately shaping a more inclusive and sustainable future for humanity.

However, rapid technological progress has ushered in a new era of interconnectedness and interdependence, where nations are increasingly reliant on digital systems and networks to power their economies and safeguard their national security. In this regard, the intersection of technological advancement and the amplification of geopolitical tensions has brought into sharp focus the myriad threats that countries face in the contemporary landscape. Among others, cyberattacks, in particular, have grown more sophisticated, transcending national borders and necessitating collaboration and partnerships among nations to protect against such threats.

These challenges have prompted all major actors – both public and private – to intensify their efforts to protect their data and digital assets. They are devising and implementing a variety of risk management strategies. The empirical evidence shows that the most effective and resilient cybersecurity policies and approaches are those tailored to specific risks and security requirements. Individual organisations need to adopt the cybersecurity measures most appropriate for the challenges they face, based on a careful risk assessment. This requires the adoption of internationally recognised cybersecurity frameworks and standards that are based upon the principles of risk management and that are relevant across sectors to strengthen consistency and continuity

Ettore Greco is Executive Vice President of the Istituto Affari Internazionali (IAI) and also Head of the Multilateralism and Global Governance programme of the institute. Federica Marconi is Researcher in IAI's Multilateralism and Global Governance programme.

among interconnected sectors and throughout global supply chains.

Cybersecurity threats are transnational by definition and as such they can be countered effectively only through global mechanisms aimed at risk reduction and trust building. A primary objective of multilateral cooperation should be the adoption of interoperable policy frameworks that promote international harmonisation and consistent cybersecurity mechanisms. The G7 can provide a fundamental impulse for this cooperation at the global level by encouraging the development and implementation of risk-based, consensus-driven frameworks, standards and risk management best practices. A commitment to these internationally recognised cyber risk management approaches and frameworks can advance economic security and enhance cyber resilience across the ecosystem.

The G7's past initiatives

Recognising the enduring and constantly shifting landscape of cyber threats at a global level, the G7 has tried to adopt measures to confront these challenges head-on, with a particular focus on the financial sector.

In 2015, the G7 Cyber Expert Group (G7 CEG) was established as a multi-year working group responsible for coordinating cybersecurity policy and strategy among G7 member countries. The G7 CEG also serves as a channel for sharing information, establishing a common understanding of the threat landscape, and facilitating incident response by implementing risk mitigation measures. To this end, the G7 CEG organises annual incident response exercises[1] and quadrennial cross-border cyber simulations. It also produces reports on specific cybersecurity issues relevant to the financial sector.[2]

In October 2016, the G7 Fundamental Elements of Cybersecurity for the Financial Sector (G7FE) were published. The objective was to enhance the resilience of the financial system by providing a set of cybersecurity practices and assisting private and public entities in developing and implementing cybersecurity policies and operational frameworks.[3] During Germany's G7 presidency, two additional reports were drawn up by the G7 CEG, setting out fundamental elements for risk management. The G7 Fundamental Elements of Ransomware Resilience for the Financial Sector contain specific recommendations for financial market agents, focusing on how they can address the increasing threat of ransomware attacks (a type of malware that prevents from accessing devices and the data stored on it, usually by encrypting files).[4]

[1] European Central Bank, *G7 Cyber Expert Group Conducts Cross-Border Coordination Exercise in the Financial Sector*, 23 April 2024, https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240423~de1afe7ceb.en.html.

[2] US Department of the Treasury website: *G7 Cyber Expert Group*, https://home.treasury.gov/node/970671.

[3] G7 Finance Ministers and Central Bank Governors, *G7 Fundamental Elements of Cybersecurity for the Financial Sector*, 11 October 2016, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf.

[4] German Federal Ministry of Finance, *G7 Countries Adopt Reports on Cybersecurity*,

IAI COMMENTARIES 24 | 22 - MAY 2024 ISSN 2532-6570

Moreover, the G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector addresses new cybersecurity risks stemming from the increasing use of service providers by financial institutions.[5] Private and public entities in the financial sector have increasingly relied on third-party relationships to support their business operations, resulting in a notable increase in the use of ICT providers in recent years. However, reliance on third parties should be coupled with robust third-party risk management to address ICT supply chain risks to individual firms. Systemic cyber risks to the financial sector may need to be addressed in a more comprehensive, holistic approach involving public and private sector stakeholders from government, supervisors, financial firms and technology companies. During Japan's Presidency in 2023, the Ministerial Declaration of the G7 Digital and Tech Ministers' Meeting, held prior to the Hiroshima Summit, addressed several important digital security issues beyond the financial sector. These included the need for international cooperation to provide secure and resilient digital infrastructure for developing and emerging economies, given their growing dependence on digital technology.

The Institutional Arrangement for Partnership (IAP) was endorsed by G7 governments at G7 Hiroshima 2023. The IAP is an international mechanism for operationalising Data Free Flow with Trust (DFFT) and represents an advancement in cross-border data flow. As today's global digital economy is fuelled by data, integrating both privacy and security measures for personal and sensitive data is paramount to safeguarding them against potential cyberattacks. Failure to do so could render them vulnerable targets for malicious exploitation.

Bringing governments and stakeholders together, IAP aims to ensure "principles-based, solutions-oriented, evidence-based, multistakeholder and cross-sectoral cooperation".[6] The IAP is hosted by OECD and is composed of the Secretariat, located within OECD, and project-based Working Groups, merging together government officials, stakeholders and experts.

Besides G7 initiatives, while comparatively limited in scope compared to them, some actions within the G20 context are also noteworthy. For example, the G20 under India's leadership adopted non-binding High-level Principles aimed at bolstering safety, security, resilience, and trust in the digital economy to support businesses.[7]

13 October 2022, https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/world/G7-G20/G7-Presidency/g7-reports-on-cybersecurity.html.

[5] Ibid.

[6] G7, *Ministerial Declaration - The G7 Digital and Tech Ministers' Meeting*, 30 April 2023, point 13, https://g7g20-documents.org/database/document/2023-g7-japan-ministerial-meetings-ict-ministers-ministers-language-ministerial-declaration-the-g7-digital-and-tech-ministers-meeting; Digital Agency website: *Institutional Arrangement for Partnership (IAP)*, https://www.digital.go.jp/en/dfft-iap-en.

[7] G20, *G20 New Delhi Leaders' Declaration*, 9 September 2023, https://g7g20-documents.org/database/document/2023-g20-india-leaders-

ISSN 2532-6570

The United Nations is another major global player. The UN Security Council convened on 4 April 2024, specifically to address cyber-related issues. Hosted by the Republic of Korea and co-hosted by Japan and the United States, the session delved into the theme of the "Evolving Cyber Threat Landscape and Its Implications for the Maintenance of International Peace and Security".[8] The discussion brought attention to the narrowing gap between low-intensity, financially motivated cybercrimes and disruptive, large-scale cyberattacks, underscoring the urgent need for further proactive measures to address these evolving threats.

Looking ahead

There are three areas in which the G7 can do more to address cybersecurity concerns. First, it can step up its support for the ongoing attempts to harmonise cybersecurity strategies between its member states with an eye to wider agreements in more inclusive bodies such as the G20 and the UN. Second, it should endorse efforts to establish common criteria to assess the trustworthiness of digital service providers that facilitate cross-border data flow. Third, in pursuing such goal, it should promote a wider and more systematic involvement of key stakeholders, including major industry actors as well as others that have expertise in cybersecurity, data protection and privacy.

Therefore, the G7 should consider undertaking further initiatives aimed at coming to a common understanding of what constitutes digital trust, with the goal of establishing a multilateral framework based on shared trustworthiness criteria. This framework would serve the purpose of addressing the cybersecurity, privacy and national security concerns while providing governments with a common basis by which to assess the trustworthiness of companies providing digital services and infrastructure such as cloud computing.

To that end, the G7 should call for the Data Free Flow with Trust (DFFT) Experts Group at the Institutional Arrangement for Partnership (IAP) to form a workstream that will focus on the technical work necessary for developing a multilateral framework on trustworthiness. It should call for the creation of an expert working subgroup within the IAP's DFFT expert group with the task of mapping out potential criteria to assess the trustworthiness of digital service providers. The G7 should also set up an ad hoc G7 group at the ministerial level to evaluate those criteria with the view of advancing and adopting a dedicated multilateral framework.

The G7 should also provide a forum for discussing and undertaking initiatives aimed at fostering cooperation among national bodies responsible for developing cybersecurity strategies. All G7 members have set up cybersecurity agencies to address

leaders-language-g20-new-delhi-leaders-declaration.

[8] Allison Pytlak and Shreya Lad, "The UN Security Council Discusses Cyber Threats to International Security", in *Stimson Commentaries*, 15 April 2024, https://www.stimson.org/?p=92869.

ISSN 2532-6570

cyber threats. Harmonising their strategies would greatly contribute to address transnational cyberattacks. The G7 should act as a key promoter of closer cooperation between national cybersecurity agencies through such activities as joint assessment of risks associated with the new technologies, sharing of best practices and coordination of standardisation efforts.

15 May 2024

ISSN 2532-6570

ISSN 2532-6570

Istituto Affari Internazionali (IAI)

The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffarInternazionali*), two book series (*Trends and Perspectives in International Politics* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17
I-00186 Rome, Italy
Tel. +39 066976831
iai@iai.it
www.iai.it

Latest IAI COMMENTARIES

Editor: Leo Goretti (l.goretti@iai.it)