Addressing the Challenges of Technological Resilience and Cyber Defense

White Paper – Cybersecurity Policy Dialogues, Aspen Technology & Society Program 2022

Radu Puchiu – Aspen Technology & Society Program Director

About Aspen Institute Romania

Aspen Institute Romania's mission is to foster values-based leadership, encouraging individuals to reflect and act in accordance with the ideals and ideas that define a good society. Using the **Aspen Method**, we provide a neutral, balanced, multi-stakeholders' venue for discussing and acting on critical issues confronting our society. Founded in 2006, Aspen Institute Romania (AIR) is part of the **international network** of like-minded Aspen Institutes around the world. **Aspen Institute Romania's work** is structured on **three main pillars of activities**: **Leadership, Policy Programs and Public Events.**

About Aspen Technology & Society Program

Launched in 2020, the **Aspen Technology & Society Program** has created a **platform for debate and a dedicated program community** composed of multiple key stakeholders from a variety of backgrounds (policy makers, private sector leaders, innovators, academic and non-governmental sector representatives) interested in subjects covering **technological developments and their impact on society**.
Aspen Technology & Society Program 2022 Program Partners: Vodafone, UiPath, Microsoft, Modex, eMAG

Introduction

In a highly interconnected world, cybersecurity plays a critical role in maintaining national security, protecting individual privacy, and ensuring the stability and reliability of critical systems and infrastructure. It protects against unauthorized access to sensitive information and systems, including personal and financial information, trade secrets, and critical infrastructure.

Being an important topic on the **Aspen Technology & Society Program** agenda, with impact on most industries, we dedicated special attention to it during our events organized in 2022. The most important ones were the ***"Digital Security Dialogue: Networks = Critical"***, organized in September and the "***Cyber Resilience and Countering Cyber Threats"*** panel at the Bucharest Forum in November.

Some of the key aspects and conclusions are described in this document as a starting point for further policy developments and proposals.

Digital Security Dialogue: Networks = Critical

The event was organized by **Aspen Institute Romania**, in partnership with the **National Authority for Administration and Regulations in Communications (ANCOM)** and with the support of the **National Cyber**

Security Directorate (DNSC), on the margins of the **ITU Plenipotentiary Conference 2022 (PP-22)** that took place in Bucharest.

Building on the role of Aspen Institute Romania as neutral, balanced, multi- stakeholders 'platform, this event was an opportunity to promote the fundamental role of ITU to build confidence and security in the use of Information and Communication Technologies (ICTs) and ITU Global Cybersecurity Agenda (GCA).

This high-level event took place under the aegis of Aspen Institute **Romania's Technology & Society** and **Resilience, Governance & Society Programs**, and facilitated a broader discussion among key players from Romania and abroad that included the public sector and institutional representatives, the private sector, academia and civil society. The distinguished speakers and panelists included:

- Houlin Zhao - Secretary-General, International Telecommunication Union
- Laura Carmen Zgonea - Secretary General, ANCOM
- Dan Cimpean - Director, DNSC
- Mircea Geoană - Deputy Secretary General, NATO (pre-recorded intervention)
- Sebastian Burduja - Minister of Research, Innovation & Digitalization, Romanian Government
- Marco Obiso - Head of the Cybersecurity Division and Acting Chief of the Digital Network Society Department, International Telecommunication Union
- Sergiu Manea - Acting President, Aspen Institute Romania
- Sabin Sărmas - President, Committee for information technologies and communications, Chamber of Deputies, Parliament of Romania
- Dragos-Cristian Vlad - President, Authority for Digitalization of Romania
- Jeff Greene - Senior Director for Cybersecurity Programs, Aspen Institute US (online intervention)
- Alexandru Mihailciuc - VP, Sales Engineering & Customer Success, UiPath
- Cătălin Buliga - Chief Networking Officer (CNO), Vodafone Romania.

Some of the key points and conclusions are mentioned below.

Building confidence and security in the use of Information and Communication Technologies (ICT)

The telecommunications industry has become one of the main driving forces behind nearly all socioeconomic activities nowadays. As the dependency on its capabilities increases, so are the attempts to interfere in them. The user experience tends to be more and more virtual, but the inevitable technological vulnerabilities therein are very real.

The OECD Recommendation of the Council on Digital Security of Critical Activities recognize that "the multiplicity and complexity of digital dependencies across sectors and borders and along critical activities' value chains create a shared digital security risk that no single actor can significantly reduce for all; that each actor is therefore dependent upon and responsible towards all others to manage digital security risk".

In nowadays context, multi-stakeholder dialogue is therefore more than critical.

Building confidence and security in the use of Information and Communication Technologies (ICT) and addressing shared digital security risks can be achieved through several best practices and policies. Some of the key approaches include:

- **Cybersecurity Awareness and Training:** Regular training and education on cybersecurity best practices, threats, and vulnerabilities can help individuals and organizations stay ahead of potential attacks.
- **Multi-Stakeholder Collaboration:** Collaboration between the government, industry, and civil society is critical in addressing digital security risks. This can be achieved through the establishment of industry-government partnerships, cross-sector collaboration, and the sharing of information and expertise.
- **Stronger Regulation and Standards:** Governments can play a key role in setting standards and regulations for cybersecurity and ensuring compliance. This can help reduce the risk of security breaches and improve overall security across the sector.
- **Investment in Cybersecurity Infrastructure and Technology:** Organizations and governments can invest in advanced cybersecurity technologies and infrastructure to improve the overall security of their systems and networks.
- **Incident Response and Disaster Recovery Planning:** Organizations and governments should develop robust incident response and disaster recovery plans to quickly respond to and recover from potential cyber-attacks.

In conclusion, addressing shared digital security risks in the ICT sector requires a comprehensive and multi-stakeholder approach that involves collaboration, investment, and education.

Governments need to work together to reduce cyber-attack related risks by implementing a coordinated approach to cybersecurity. This includes:

- **Sharing threat intelligence:** Governments can share information about the latest cyber threats, their sources and their methods of attack. This will help in creating a shared understanding of the threat landscape and improve preparedness.
- **Developing common standards:** Governments can work together to develop international cybersecurity standards and regulations to ensure the security of critical infrastructure and sensitive data.
- **Improving incident response:** Governments can collaborate on incident response procedures to ensure that cyber incidents are effectively dealt with, and the impact of these incidents is minimized.
- **Enhancing legal frameworks:** Governments can work together to develop harmonized legal frameworks for cybercrime and improve international cooperation in the investigation and prosecution of cybercriminals.
- **Promoting international cooperation:** Governments can encourage the formation of international partnerships and collaborations between the public and private sector to strengthen cybersecurity.

By working together, governments can effectively address the growing threat of cyber-attacks and reduce the associated risks to individuals, organizations, and national security.

The cybersecurity challenges large network providers face

Large network providers face several challenges when it comes to cybersecurity:

- **Complexity of networks:** With the increasing complexity of networks, it becomes difficult to identify and secure all potential entry points for attackers.
- **Evolving threats:** Cybersecurity threats are constantly evolving and becoming more sophisticated, making it challenging for providers to keep up and ensure their systems are secure.
- **Supply chain vulnerabilities:** The supply chain for many technology products and services is global and often difficult to monitor, making it difficult for providers to identify and mitigate vulnerabilities introduced by third-party components.
- **Increasing number of devices:** The increasing number of connected devices, such as IoT devices, exacerbates the security challenge for network providers as it increases the number of potential entry points for attackers.
- **Regulation and compliance:** Network providers must comply with a growing number of regulatory requirements related to cybersecurity, which can be time-consuming and expensive.
- **Balancing security and privacy:** Network providers must balance the need for security with the need to protect the privacy of users and their data. This can be challenging, as many security measures can affect user privacy.

Cybersecurity at the Aspen – GMF Bucharest Forum

The 11th edition of the **Aspen – GMF Bucharest Forum** - the flagship event organized by the **Aspen Institute Romania** and **German Marshall Fund** - was focused on the societal impact of disruptive new technologies and the complex issues of an increasingly dynamic and volatile international context. The conversation addressed both of these areas to ensure societal resilience in the West.

On the dedicated panel at the event, entitled **Cyber Resilience and Countering Cyber Threats**, organized in partnership with Aspen Institute US & Aspen Germany, we had the pleasure of welcoming:

- Jeff Greene, Senior Director for Cybersecurity Programs, The Aspen Institute; Former Chief for Cyber Response & Policy, National Security Council, White House (by video conference)
- Jeff Bullwinkel, Regional Vice President, Corporate External & Legal Affairs, Microsoft Europe
- Chelsey Slack, Deputy Head, Cyber and Hybrid Policy Section, NATO Headquarters
- Dan Cîmpean, Director, National Directorate of Cyber Security (DNSC) (by video conference)
- Arthur Lazăr, Deputy Director, Cyberint Centre, Romanian Intelligence Service.

Cybersecurity was quite high on the agenda and the panel analyzed challenges posed by new technologies, looking in particular at improving resilience in the context of technology-related threats, especially when it comes to trans-Atlantic cooperation.

Some of the key take-aways from Aspen – GMF Bucharest Forum were included in the ”A World in Flux – Towards a New European Architecture Report” having as distinguished contributors, among others, Mircea Geoana, Deputy Secretary General of NATO, Christoph Heusgen, the Chairman of Munich Security Conference, Maroš Šefčovič, the European Commission Vice-President for Inter-institutional Relations and Foresight, Marta Dassù, Senior Advisor for European Affairs, Aspen Institute Italia, Helga Maria Schmid, OSCE Secretary General, and many more.

On cybersecurity and resilience, Radu Puchiu, Director of the Technology and Society Program, Aspen Institute Romania, highlighted in the same document some of the key areas that need to be addressed:

- **Unity of the West on Tech:** The war in Ukraine accentuates the need for strategic autonomy on critical technologies in the West. While the EU has taken steps to protect user rights and create a level playing field for businesses, there is still a fragmented approach to the issue. A more coherent collaboration is needed to address the tech vulnerabilities of Europe and the West.
- **A Broader Approach to Resilience:** Europe's strengths and weaknesses are a result of its member's actions. To address these vulnerabilities and contribute to the resilience of the West, a common technology agenda from a broader perspective is mandatory. Local tech efforts should be aligned with the greater goal of unity and prosperity.
- **Joint Cyber-Defense:** As our dependency on infrastructure and data increases, so does the risk of digital vulnerabilities. The EU's quest for digital sovereignty should be aligned with international cyber collaboration to effectively manage digital security risk.

Cybersecurity Context

Cybersecurity has a long history that dates back to the early days of computing. One of the earliest recorded cyberattacks was the "Morris worm" in 1988, which infected thousands of computers connected to the

Internet. Since then, the threat of cyberattacks has grown dramatically as the number of connected devices has increased and the complexity of computer systems has grown. In response to this growing threat, the field of cybersecurity has evolved and matured. The development of new technologies and best practices, such as firewalls, encryption, and threat intelligence, has helped organizations to better protect their systems and data. Governments around the world have also developed policies and laws aimed at improving cybersecurity and protecting citizens from cybercrime.

However, despite these efforts, the threat of cyberattacks remains high. In recent years, we have seen numerous high-profile breaches and cyberattacks, including the WannaCry ransomware attack, the Equifax data breach, and the SolarWinds supply chain attack. These events have demonstrated the need for continued investment in cybersecurity research and development, and the importance of staying vigilant in the face of an ever-evolving threat landscape.

Cyber-attacks can affect people of any age, gender, or socioeconomic status, as the use of technology and the internet has become widespread and increasingly ubiquitous in our daily lives. However, some groups may be more vulnerable to cyber-attacks than others, such as older individuals who may not be as familiar with technology, low-income individuals who may not have access to resources to protect themselves online, and individuals from marginalized communities who may be targeted for their identities. It's important to note that cyber-attacks can have varying levels of impact on individuals based on their age, gender, and socioeconomic status, and a comprehensive analysis would require more specific data and research on each particular population.

The impact of a cyber-attack can be widespread and far-reaching, affecting individuals, businesses, and governments. The consequences can include financial losses, loss of sensitive or confidential information, reputational damage, and even disruption to essential services such as healthcare, transportation, and energy.

The war in Ukraine

The Russian invasion of Ukraine faced a strong and unitary answer from Western democracies. It led the once-divided European Union to unite behind sanctions against Russia - a more coherent collaboration between the US and the EU, politically and militarily.

Microsoft presented "Defending Ukraine: Early Lessons from the Cyber War"[1] which gathered an important view on the importance of cybersecurity and how collaboration is key in such times. There are valuable lessons to be learned from Ukraine's experience with cyber-attacks. The article highlights that Ukraine has been at the forefront of a new type of warfare, one that is waged in cyberspace, and as a result has had to develop new strategies to defend itself. The authors argues that the experiences of Ukraine in dealing with these attacks can serve as a model for other countries facing similar challenges. The article highlights the need for increased collaboration and information sharing between countries, as well as the importance of investing in the development of strong cybersecurity infrastructure and the development of a skilled workforce. Ultimately, all of these underline the idea that countries must work together to address the common threat posed by cyber-attacks and to develop effective strategies for defending against them.

Conclusions

A general conclusion from the discussion is that addressing the challenges of technological resilience and cyber defense requires collaboration and a common approach. The vulnerabilities of Europe and the West should not become a weakness, but rather a strength through a unified effort to ensure a secure and prosperous future.

We also noted some important possible **policy approaches**:

- The West must address the issue of unity on tech as a priority and work towards a more coherent approach in dealing with critical technologies.
- The EU should broaden its approach to resilience and address the vulnerabilities of member countries as part of the larger coalition of democracies in the West.
- The EU must align its quest for digital sovereignty with international cyber collaboration and engage in joint cyber-defense efforts.
- Countries must establish a task force composed of experts from various fields to assess the vulnerabilities and recommend measures to address them.
- Foster partnerships between the EU and tech giants to collaborate on key initiatives that support the development of a more secure digital space.
- Encourage EU member countries to invest in digital infrastructure and digital education, to close the digital gap and improve their overall competitiveness in the digital economy.
- Develop and implement a comprehensive cyber-defense strategy that involves regular assessments of the EU's digital security risk and the development of mitigation measures.

In terms of the economy, the cost of cyber-attacks can be substantial. According to various reports, the cost of cybercrime globally is estimated to be hundreds of billions of dollars each year and is projected to continue

[1] https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

to rise. These costs include direct financial losses, such as from theft or fraud, as well as indirect costs, such as from lost productivity and revenue due to disrupted operations. Additionally, organizations may incur costs related to recovery and mitigation efforts, such as hiring cybersecurity experts and upgrading security systems.

Some examples of research studies that demonstrate the magnitude of cyber attacks:

- "Microsoft Digital Defense Report 2022": unique insights on how the digital threat landscape is evolving and the crucial actions that can be taken now to manage the risks.
- "Cost of Cyber Crime Study"[2] conducted by the Ponemon Institute: This study provides an estimate of the annual cost of cybercrime for organizations in various countries and industries.
- "Global State of Information Security Survey"[3] conducted by PwC: This study provides insights into the current state of cybersecurity and the impact of cybercrime on organizations globally.
- "Economic Impact of Cybercrime"[4] report by the Center for Strategic and International Studies (CSIS): This report provides a comprehensive analysis of the economic impact of cybercrime, including the cost of data breaches and cyber-attacks to organizations and the global economy.

These studies demonstrate the magnitude of the cyber-attack problem and highlight the need for organizations to invest in robust cybersecurity measures to protect themselves against cybercrime.

In terms of best practices and successful policies that have been implemented to mitigate the impact of cyber-attacks participants mentioned:

- **National Cybersecurity Strategies:** Many countries have developed national cybersecurity strategies that outline the key policies and measures to be taken to protect their national security and critical infrastructure.
- **Cybersecurity Information Sharing Act (CISA):** This is a US legislation aimed at improving cybersecurity information sharing between the government and private sector organizations. The act encourages organizations to share information about cyber threats with the government, while protecting their sensitive information.
- **Cybersecurity Certification Schemes:** Some countries have established cybersecurity certification schemes to help organizations assess and improve their cybersecurity posture. The certification schemes often require organizations to meet certain security standards and undergo regular security audits.
- **Incident Response Plans:** Effective incident response plans are essential for organizations to quickly and effectively respond to cyber-attacks. These plans outline the procedures and responsibilities for detecting, containing, and mitigating cyber threats.
- **Security Awareness Training:** Regular security awareness training can help organizations educate employees on the latest cyber threats and how to avoid them.
- **Investment in Cybersecurity Research and Development:** Governments and private sector organizations should invest in cybersecurity research and development to develop new security technologies and solutions to stay ahead of evolving cyber threats.

[2] https://www.ponemon.org/research/ponemon-library/security/2017-cost-of-cyber-crime-study.html
[3] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html
[4] https://www.csis.org/analysis/economic-impact-cybercrime

These are just a few examples of best practices and successful policies that have been implemented to mitigate the impact of cyber-attacks. The specific approach might vary depending on the nature and scale of the threat, as well as the resources and capabilities of the organization or government.

The main conclusions of the above are that the digital technology is a crucial enabler of modern day socioeconomic activities, but is also subject to increasing interference attempts due to its vulnerabilities. There is a shared digital security risk across sectors and borders, and a multi-stakeholder dialogue is critical to address this. Building confidence and security in the use of ICT requires governments to work together, while large network providers face challenges in terms of cybersecurity. The OECD Recommendation recognizes the need for a shared responsibility to manage digital security risks.