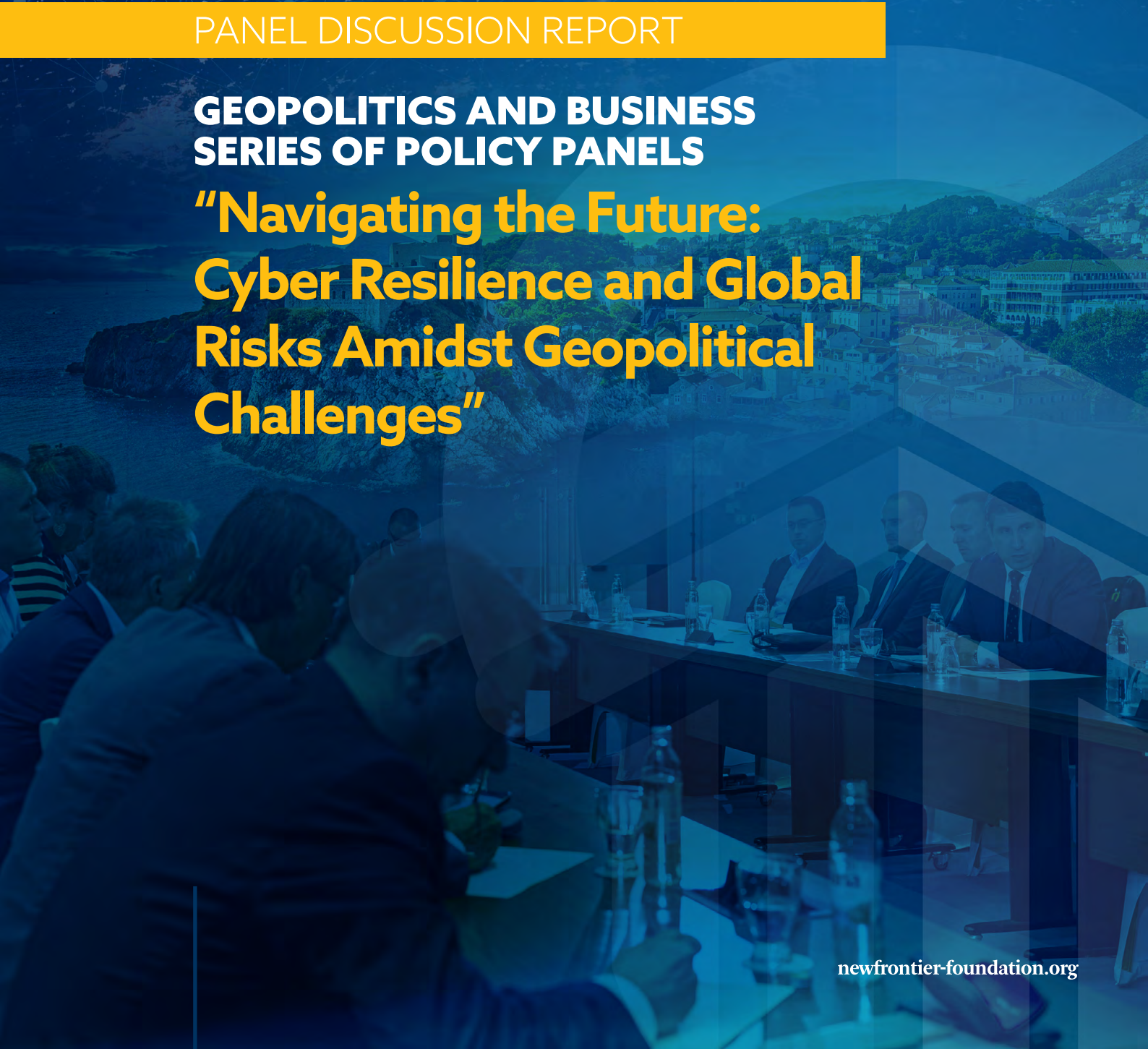
New Frontier
FOUNDATION

PANEL DISCUSSION REPORT

GEOPOLITICS AND BUSINESS SERIES OF POLICY PANELS

"Navigating the Future: Cyber Resilience and Global Risks Amidst Geopolitical Challenges"



newfrontier-foundation.org

The roundtable discussion on „Cyber resilience and global risks amidst geopolitical challenges" organized in Dubrovnik, Croatia on 27th June 2024, by the New Frontier Foundation , brought together eminent national, and European experts in the field of cybersecurity. Keynote presentations by representatives from the private sector provided an overview of the challenges and experiences faced by a leading Croatian IT company and a leading global technology company in online payments. The discussion highlighted current and future risks, challenges, and needs of both public and private sectors in the fight against growing cybercrime.

Introduction

The discussion was more than timely given the recent cyberattacks on government institutions and the biggest hospital in Croatia. These attacks demonstrate that the global security environment is in a dynamic change with multiple complex and interdependent threats, accelerated by the revival of power politics, empowered with modern technologies and often hybrid in its nature. During the debate panelists addressed the following key topics:

- Main cybersecurity trends, challenges and threats for the region;
- European cybersecurity regulatory landscape;
- Tools for societies, businesses and governments to apply to ensure resilience against cyber threats.

State of play

Spurred largely by artificial intelligence and automation, the fourth industrial revolution has brought the development of new digital technology, whose speed and plethora of innovations simultaneously carry not so long ago unimagined potentials and risks, if left unregulated and in the hands of the ill-intended. As technology rapidly advances, so has the diversity and quantity of cyberattacks across the globe. To address these threats, the European Union (EU) has taken a leading stance in adopting legislation aimed at fostering a common level of cybersecurity across the EU. Recent examples include the AI Act, the NIS2 Directive , as well as the Digital Operational Resilience Act (DORA). While legislation in the field is essential, close collaboration and exchange of best practices between the private and public sectors on cybersecurity is equally important, as is engaging in wide public awareness campaigns aimed at protecting citizens and businesses against cyberattacks.

Corporate perspective

While IT advancements, the internet, mobile devices, and networks have revolutionized our world, they also present serious challenges, as these powerful tools can be wielded for both positive and negative purposes. Cybercrime is an industry enabled by digitization and connectivity, allowing illegal earnings generated in the virtual world to be converted into real money. This possibility was introduced in 2008 with the development of blockchain and cryptocurrencies. Tracking movements and transactions in cryptocurrencies is challenging for governments, especially when the payout location is far from a developed society and functional legal system.

Experts estimate that the costs associated with cybercrime worldwide in 2022 have reached a staggering $6 trillion, equivalent to 1% of the global GDP. While this amount may not seem large, the economic damage is comparable to that caused by climate change in the same year. From 2020 to 2023, the number of cyber-attacks has increased by staggering 600%. Additionally, the loss per each data breach is estimated to be 4.5 million USD. The cybercrime has grown in a very powerful and lucrative illegal industry with an annual growth rate of 15%. The impact of damages from 2022 to 2023 exceeded 1% of global GDP and grows annually between 2.5% to 4.5%. Furthermore, the low conviction rate for cybercriminals stands at just 0.05%.

Everyone should be aware that cyber-attacks do happen. Companies operating in this field face dozens to thousands of attacks daily and employ large teams of top experts who work on security measures, and have predefined protocols, and procedures for handling cyber-attacks.

The corporate sector is making efforts to drive positive change in the market and assist the government sector. But, it is faced with risks such as lengthy administrative procedures and procurements that can cause delays in maintaining IT systems and their security, making them an easy target for cybercriminals.

The corporate sector, especially the sector dealing with payments and transactions, actively collaborates with international bodies and government agencies in the countries where they operate, such as the National banks, FBI, Europol, or Interpol. Additionally, the private sector invests significant resources in security and client education and awareness raising, particularly for young people entering the world of transactions and investments.

In Croatia, companies share information about attacks with each other and with the Government, thus assisting in the collective fight against cybercrime. Given today's level of interconnectedness, security systems must be developed at an economy-wide level, not solely within individual companies, to effectively combat cybercrime.

The corporate sector rightly expects support from regulators at the EU level. Additionally, the corporate sector advocates for deeper collaboration among institutions, national banks, and regulatory bodies

in data, knowledge and exchange of best practies, as well as a stronger deterrent role from legislation, law enforcement agencies, and the judiciary. Such collaborations are underpinned by three key principles: safety, security and trust.

Institutional perspective

The public sector considers collaboration with the private sector crucial, as well as cooperation among institutions and government organizations across Europe and the world. Countries establish various national working groups and organizations, and institutions collaborate with the corporate sector. Romania for example has recognized the importance of aligning the work of national bodies and has established a dedicated entity tasked with combating cybercrime. The system they are building includes specialized regulators for cyberspace, intelligence agencies, the Ministry of Defence, and the Ministry of Internal Affairs, while also providing training for experts. There is also significant support from EU funds for the establishment of such a system.

To effectively protect cyberspace good cooperation at all levels of society is needed. The introduction of different ideas and approaches from SMEs, based on the type of business, activity, or problem to solve is needed. Investment in human resources, awareness raising, and education of the broad public is needed. New insurance products are also seen in the market like cyber insurance. However, without the collaboration of the public sector with the corporate, the results would not come close to what they achieve. The private sector provides data on attacks, and in cooperation with experts, they prepare and provide appropriate responses.

Since the beginning of the war in Ukraine, a significant increase in cyber-attacks from Russia has been recorded. Also, there is an increasing number of attacks on SMEs, who are more vulnerable because their budgets for protection are not substantial. Simultaneously, young hackers engage and use small SMEs as "target practice" before moving on to harder and bigger objectives.

Furthermore, changes and technological advancements are evident in the methods used for cyber-attacks. Securing cyberspace is far from easy. In 2014 and 2015, seventeen Member states were targeted, and external domain registries were breached. The attack lasted for months.

One can easily predict that attacks will become increasingly sophisticated, and the situation will worsen. Therefore, it's essential to be proactive rather than reactive. Acting in advance is crucial.

On the national level, the Croatian government launched the SK@UT pilot project due to the increased number of APT cyber-attacks on Croatian infrastructure. Today more than 80 entities are included in this cyber security system. At the EU level, Croatia collaborates on connecting national systems and data exchange. At the global level, Croatia participates in the Rosenberg Initiative. In the context of cybersecurity, this initiative aims to counter cybercrime and promote responsible use of information

and communications technology (ICT). So far, more than 50 states have joined this initiative.
Today, we are witnessing an open war between Russia and Ukraine in all domains, including cyber warfare. Most cyber-attacks are linked to espionage. However, some attacks serve as mere decoys and distractions, concealing much more serious threats underneath (such as data theft, data destruction, or ransomware).Russia is certainly a haven for cybercriminals. After the start of the war with Ukraine, cybercrime organizations fragmented due to divergent interests, leading to data leaks. It has been observed that such states shift their activities to criminal groups. Notably, protocols for defending against cyber-attacks are emerging within the criminal milieu.

In the future, we can expect an increasing presence of generic technologies (such as 5G as a generic IT technology). In about 5 years, telecom protocols (which hackers are unfamiliar with today) will disappear, Wi-Fi will become obsolete, and 5G and 6G networks will replace them. As the transition to 5G technology intensifies, the situation will only worsen. Therefore, for effective defense against cyber-attacks in the 5G environment, it will be necessary to further develop coordination between the public and private sectors and introduce automatic data exchange.

Discussion

State-sponsored attacks are just the tip of the iceberg. The real challenge lies in the unstoppable growth of cyber criminals. However, part of the blame for these issues should be recognized on our side. Firstly, inadequate data hygiene is the cause of approximately 70% of cyber-attacks. Delays in applying patches account for about 20% of successful cyber-attacks.

Companies often claim that data protection for their clients is a priority, but we can witness that investments in cybersecurity fall far short of what is necessary. Considering an initiative to increase penalties for the theft of sensitive data could encourage firms handling such data to invest more. People are vulnerable, and this vulnerability is increased by human tendency to frivolously trust one another.

The system should protect the most vulnerable, so those profiting from storing citizens' sensitive data should bear the burden of security costs. Therefore, those who provide services are the only ones who can control and protect users, as long as the users are not fraudsters or extremely irresponsible. System security should be ensured by design and clearly communicated to the user, rather than hidden in the small letter of disclaimers that users sign in contracts.

The EU is currently striving for greater user protection, especially for retirees who are frequent and easy targets. Notably, there hasn't been a significant breach of security of the banking system so far. It is encouraging to note that bank security has been at a high level, and banks are better protected than SMEs.

Crypto assets seem to enable cybercrime to be a successful business. There are different approaches to this issue, ranging from complete removal from the EU market to more liberal approaches. However, member states should maintain a joint approach and align with the Digital Operational Resilience Act (DORA).

Cash is still the primary means of payment when it comes to criminal activities. Insurance companies, in response to this type of threat, offer coverage for damages caused by cybercrime through 'cyber insurance.' The situation is challenging, and everyone should be much more cautious. Insurance companies align their operations with DORA and apply a risk-based approach within their departments. Just like with other lines of insurance, they employ specialists to assess risks and handle damages resulting from cybercrime.

The corporate sector must establish a good balance between risk and investments. IT companies offer complex services such as security centers but also provide protection services for smaller firms. For successful awareness-raising in the corporate sector, initiatives are necessary. In certain EU funding programs and at the national level, co-financing investments in IT infrastructure already require investment in cybersecurity. There should be more of that.

Technical inspections need to be introduced for companies that work with IT systems, following well established common practices like annual vehicle inspections. In the bank sector in depth audit already exists but is not standardised. Also, the development of new and new layers of security to tackle even newer threats are very different and complex, leaving gaps and holes. A new approach to cyber security needs to be simple and versatile.

Conclusions and recommendations

How to effectively protect cyberspace?

- Engage with SMEs: Involve subject-matter experts (SMEs) in developing tailored solutions based on specific job types.
- Invest in Expertise: Allocate resources to invest in cybersecurity experts.
- Educate Users: Educate cyberspace users about security measures.
- Vulnerability Discovery: Encourage the identification of weak points and reward those who report security flaws (like Microsoft's approach)

How to effectively protect yourself from cyber-attacks?

- Strong Passwords: Use complex, unique passwords for your accounts and change them periodically.
- Software Updates: Regularly update your software to patch vulnerabilities.

- Think Before You Click: Be cautious when clicking on links or downloading attachments in emails or messages.
- Multi-Factor Authentication (MFA): Enable MFA for an extra layer of security.
- Control Network Access: Limit who can log on to your network and use your devices.
- Data Encryption: Encrypt sensitive data both at rest and during transmission.
- Regular Backups: Back up your data to prevent data loss.
- Risk Assessments: Conduct annual risk assessments to identify vulnerabilities.
- Access Control: Clearly define and assign information security roles.
- Third-Party Audits: Have reliable third-party audits of security control

How to effectively protect yourself and your customers in case of a data breach?

- The first level of response is always to disconnect from the outlet.
- Cyber-attacks should be reported to the authorities.
- Collect all data about the cyber-attack.
- Analyse data.
- Develop relevant protocols and procedures.
- Provide notifications on risks, breaches, how to prevent similar attacks and limit the damage.

Dubrovnik, Croatia on 27th June 2024