POLICY BRIEF

CYBER

Cyber (In)Security in 2022

OVERVIEW

With the onset of Industry 4.0, the rapid evolvement of digital environment and intense digitalization of the world, the importance of cyber field is undeniable. When observing state institutions, it is vital to take into consideration both physical and online dimensions. Government online institutions are under the biggest risk since they are the major holders of vital resources and databases which can influence various processes in the country. What can be said about cyber security in 2022? Do countries contribute enough to the development of the cyber niche, providing a reasonable degree of protection for government structures, ensuring the security of data for their citizens? In our policy brief we will pinpoint critical cases within this topic, analyze past mistakes and suggest ways for further improvements to be made.

Despite the fact that the topic is extremely broad, we will concentrate on the two specific cases of Ukraine and Lithuania since they demonstrate the present importance of cyber protection for states. The moment not just a full-scale invasion but a war started in Ukraine, it was clear that government structures and databases were prone to attack. The number of cyberattacks increased significantly, leading to the necessity of implementing additional security measures in order to protect both citizens' personal information and government resources.

To add more, someone may argue there are already established organizations which are responsible for the cyber security issue, such as the UN General Assembly[1] or UN Security Council UNSC, however, their resolutions are more or less recommendatory and non-binding on member states. That is why we need improvements of institutionalization processes on a national security level to not only deal with the consequences, but also in order to prevent possible cyber conflicts nowadays and in the future.

Key points:

- cyberattack as a manipulation tool
- importance of established and not yet created organization in ensuring the needed level of cyber security
- vulnerability of cyber infrastructure as an open door for unfriendly actors' sabotage
- imposed goals of cyberattacks: damage to databases, possession of information or psychological influence on society
- common legal framework as major upgrade to the level of international importance

Authorship: Diana Makedon, Mariia Hlyten, Rastsislau Marozau, Alina Evstratikova - participants of JLU-EHU-KAS exchange program

Publication date: August 2022

1-In Hindsight: The Security Council and Cyber Threats, 2020

KONRAD ADENAUER STIFTUNG BELARUS

JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN

EHU European Humanities University

Killnet Case in Lithuania

On 27 June, Lithuanian government websites related to government and city infrastructures were attacked[2] by a group of Russian killnet hackers in response to a ban on imports of cargo from Kaliningrad through Lithuanian territory. “The attack will continue until Lithuania lifts the blockade,” a Killnet spokesperson said. “We have demolished 1,652 web resources. And that's just so far.”
“It is very likely that attacks of similar or greater intensity will continue in the next days, especially in the transportation, energy and financial sectors,” Lithuania's National Cyber Security Centre said in a statement following the attack.

This is not the first time a group of hackers on Russia’s side has hacked state cyber infrastructure[3]. Czechia, Moldova, and Romania have also fallen victim, however this is not a complete list of the countries targeted. Why are such groups so effective that, despite their lack of funding and other resources, they are able to hack well-protected government websites, penetrating the protection of state cyber institutions? The vulnerability of cyber infrastructure may not seem like a high priority in peacetime, but during regional and international conflicts, this vulnerability opens up many opportunities for unfriendly actors to influence not only single individuals, but also entire cities and countries. In today's era, when many fundamental aspects of life are integrated within the internet infrastructure, every cyberattack has a huge impact on vast groups of people.

In the case of the cyberattack on Lithuania, authorities were able to respond quickly to the attack and resume normal operation of critical infrastructures. But the very existence of this attack shows that at any moment, every person in the country can become a victim of this vulnerability, and critical decisions must be made at the national level to protect cyber infrastructure and safeguard people’s data.

As both Lithuania and Ukraine were rapidly developing their cyber fields and both suffered the consequences that came with the swift growth, we decided to showcase the **cyberattacks aimed at government infrastructures** in these countries.

Diia Case in Ukraine

What is the cyber security situation in Ukraine? In January 2022 a massive cyberattack took place on Ukrainian government institutions and the online app “Diia” released by the Ministry of Digital Transformation of Ukraine[4]. Although the platform was restored within 3 days and no sensitive information was leaked, the pressure was evident. The goal of the well-prepared cyberattack, most probably organized by a group of Russian hackers as the Ukraine’s Security Service revealed, was not just the destruction of critically important government online resources and access to the vital information, but also to influence the Ukrainian public. Shortly after the attack, rumors spread regarding the leakage of personal data of thousands of Ukrainians from the database of “Diia”. The data was announced to be sold via darknet resources that crested trust issues between Ukrainian society and its government[5].

2-Lithuanian government. Information of Ministry of National Defence of. Intense DDoS attacks targeted several companies and institutions in Lithuania . 2022.

3-Sytas, Andrius. «Russian group claims hack of Lithuanian sites in retaliation for transit ban.» Reuters (Reuters), 2022.

4- Government, Ukrainian. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року. Kyiv, 2020.

5-BBC. Ukraine cyber-attack:Russia to blame for hack, says Kyiv, 2022.

Recommendations:

1. IDENTIFY KEY CYBER ACTORS: **Which organization or state will be responsible in the event of a cyberattack?** Who might be taken as a guarantee of safety? The procedure of recognition of cybercrimes must be institutionalized as well as the responsibility of certain authorities.

2. RISK MANAGEMENT: **All possible scenarios are to be estimated**. By knowing the major problems, we can prepare in advance to prevent cyberattacks or, at the very least, reduce their consequences. Computer emergency response teams[6] might be organized as a response to cyber threats for a quick reaction to possible attacks as Estonia has once implemented it. There are some system check-ups led by those teams which helped the state prevent a further 300 possible cyber-attacks on vital services.

3. CREATE NEW REGULATIONS: **Common legal framework must be established.** These need to be shaped as well as the question regarding cyber security needs to be promoted to international prominence since cyberattacks are used as a tool of manipulation during wars. Moreover, there must be a common understanding of cyber security at all levels – states, private organizations as well as citizens. Mutual understanding must be provided in order to overcome cyber (in)security difficulties successfully.

4. IMPROVE INFORMATION SHARING AND SENSING: As a useful tool, a new legal framework must be ensured to **provide robust solutions** to the listed challenges or possible problems and difficulties which might occur. The cooperation between authorities and society regarding cyber safety rules and regulations must be added and considered. Estonia's level[7] of cyber security can be taken as an example of one of the most developed countries in this field.

5. ENHANCE COOPERATION AND SECURITY AMONG STATES: Referring to possible options for further cooperation and security among countries, the opinion of Mischa Hansel, Head of "International Cybersecurity" research at the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH) can be taken into consideration. He argues that we can **create like-minded states communities[8]** to promote an international wealth and security.

6-Cybersecurity, the European Union Agency for ENISA Mandate and Regulatory Framework. 2019.

7-Communacations, Ministry of economic affairs and. CYBERSECURITY STRATEGY: Estonia. 2019-2022.

8-Hansel, Misha. Cyber-attacks and IR psychological perspectives: explaining misperceptions and escalation risks. Hamburg: Journal of International Relations and Development 21(3): 523-551. DOI: 10.1057/s41268-016-0075-8, 2018.

Overview-Nazli Choucri, Stuart Madnick, Priscilla Koepke. Institutions for Cyber Security: International