NCSCC
NATIONAL CYBERSECURITY COORDINATION CENTER

USAID
FROM THE AMERICAN PEOPLE

ICWR
INSTITUTE OF CYBER WARFARE RESEARCH

EXPECTATIONS AND REALITY OF CYBER WARFARE

WHAT UKRAINE FACED AND HOW IT RESPONDED TO CYBER AGGRESSION

The study "Expectations and reality of cyber warfare. What Ukraine faced and how it responded to cyber aggression" was made possible through support provided by the U.S. Agency for International Development within the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

NCSCC
NATIONAL CYBERSECURITY
COORDINATION CENTER

USAID
FROM THE AMERICAN PEOPLE

ICWR
INSTITUTE OF CYBER WARFARE
RESEARCH

CONTENTS

INTRODUCTION

The purpose of this research was not to create a new analysis of lessons learned from the cyber warfare, but to focus on the direct experience and expectations (and therefore the quality of planning) of Ukrainian cybersecurity professionals and the cybersecurity situation they actually faced after the 24th of February 2022. This aspect is important, as understanding the quality of cybersecurity policy planning at both the state and individual organizations' levels allows us to better understand an urgency of challenges the state was preparing for in the context of active cyber warfare, and what specific steps were taken to prevent escalation, as well as the current cybersecurity situation in the country.

PREVIOUS RESEARCH ON LESSONS LEARNED FROM CYBER WARFARE

Since the first months of the Russian invasion, experts have been trying to assess, on one hand, an impact of a cyber component on the military-political situation and peculiarities of the conflict (for example, the works “Cyber Front. How Russia Attacks Ukraine and Are We Ready to Defend Ourselves”[1], “Russia’s War in Ukraine: The War in Cyberspace”[2], “Defending Ukraine: Early Lessons from the Cyber War” [3], “An Overview of Russia’s Cyberattack Activity in Ukraine”[4] or discussions during CYBERUK 2022 in May 2022), and on the other hand, to determine at a general level what strategic lessons can be learned from the cyber warfare between Russia and Ukraine.

The first assessments of dynamics of the cyber warfare indicated low variability of Russian cyberattacks (mostly traditional DDoS and phishing as a basis), no noticeable effect on the operation of Ukrainian critical infrastructure facilities (an exception is a case of a cyberattack on VIASAT and, as it became known later, several attempts to use pyros to attack the energy sector), and cyber activities in close cooperation with the special services of Republic of Belarus. The first months of the confrontation also showed the following:

✓ IT systems important for a vital activity of the state were not disrupted;

✓ Ukrainian and international cyber experts managed to counteract a number of facilities in Russia, stealing data from numerous Russian companies and organizations (including data on Russian military personnel involved in the war against Ukraine);

✓ an ability to counteract cyberattacks depends more than ever on an effective international cooperation;

✓ cyber threat intelligence and EDR implementation have significantly aided to counteract destructive cyber threats;

✓ Russia understands an importance of disrupting the unity of its partners, so it attacks not only Ukraine but also its allies;

✓ cyber espionage is still a significant element of cyber activity, although an impact of cyberattacks during the conflict was expected to be more devastating.

Forecasts in April 2022 indicated that cyberattacks against Ukraine would only intensify, and that Russian nation state cyber actors would actively move beyond Ukraine and the conflict area[5].

[1] Cyber Front. How Russia Attacks Ukraine and Are We Ready to Defend Ourselves // https://biz.nv.ua/ukr/experts/kiberataki-rosiji-na-ukrajinu-yak-prohodyat-ta-chim-zagrozhuyut-ostanni-novini-50236927.html

[2] Russia’s War in Ukraine: The War in Cyberspace // https://icds.ee/en/russias-war-in-ukraine-the-war-in-cyberspace/

[3] Defending Ukraine: Early Lessons from the Cyber War // https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/?fbclid=IwZXh0bgNhZW0CMTEAAR3n7BOFahiVi_nGsrHVfexR4Gh7_MDMYBRvNxolQBI6f1RRq5u3GRAlXQk_aem_AaGO9RmBwcq2yg-ID_weJVJhiCZdO0gk4ljzztt76nG9Cw64AqJuceSA_1QvMua1coKU-7vB4dBwgtGdb9GrOgJ2

[4] An Overview of Russia’s Cyberattack Activity in Ukraine // https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[5] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

The first overall assessments of the situation (mostly by Western think tanks or officials) and cautious formulations of lessons of cyber warfare began to appear only in autumn 2022. These assessments include:

✓ **October 2022.** Rob Joyce, Director of Cybersecurity at the US National Security Agency (NSA), comments on the Russian-Ukrainian cyber warfare[6] with a focus on an importance of public-private partnerships, joint work with intranational partners and the need to develop resilience skills**.**

✓ **December 2022.** Analysis by Carnegie Endowment For International Peace[7]. An analyst of the center offers a comprehensive look at the impact of Russia's cyber operations against Ukraine since the invasion. The main conclusion is that operations had no strategic impact, but there are also no lessons that other countries can learn.

✓ **January 2023.** Analysis of the situation from the specialized publication Breaking Defense. The general analysis of reasons for failures of Russian cyberattacks in Ukraine and how it relates to an international assistance provided[8].

✓ **February 2023.** Mandiant's assessment of the first year of cyber warfare[9]. Emphasis on a noticeable politicization of cybercrime groups regarding to the Russian-Ukrainian warfare, as well as forecasts of intensified information operations combining PSYOP and cyber components, not only against Ukraine but also its allies.

✓ **February 2023.** ESET's research on a role of wipers in the Russian-Ukrainian cyber warfare[10]. The main conclusion is that cyberattacks with wipers are nothing new for Ukraine, although it is difficult not to note a significant increase in dynamics of their use since February 2022.

✓ **February 2023.** The European Cyber Conflict Research Initiative (ECCRI) has prepared a report "The Cyber Dimension of the Russian-Ukrainian War", which, in addition to already provided assessments of a nature of the cyber conflict, focuses on a role of cyber activists on both sides and a blurred status of cyber activists in modern conflicts.

✓ **March 2023.** Microsoft Assessment[11] , which determines a factor of wipers in the first year of the warfare (at least 9 new families), also points to a new noticeable track of Russian cyber activity – more attacks against allied countries with espionage purposes.

[6] https://www.infosecurity-magazine.com/news/nsa-6-takeaways-war-ukraine/?fbclid=IwZXh0bgNhZW0CMTEAAR0uikj7syNknUvPyYNxrwtqCx-iDBzPYqX7M9P5awvJ_4K7Fye0cWzhtAqE_aem_AaFB_BtyRIvNLwDDx5IRecc_mITNUWEbtE95aWeCmFmmguW5hqFUrJBdRwaVTsFWEj002sxeO-JpEIuUDNin_AZ5c

[7] https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en

[8] https://breakingdefense.com/2023/01/no-big-bang-cyber-successes-in-ukraine-are-no-cause-for-complacency-in-us/?fbclid=IwZXh0bgNhZW0CMTEAAR0HhLJuJ1rPeBHTRiK2iy-ndxmVU3BEtmPTqHgzYFi6afG9xzAw0TuvkfM_aem_AaF8zPdmVzRutnKz0XhJOaz_Vs-FARz-7N_e3tQnl8lf_7wsicuBPlJuQz00oE28XlsaERAJHuNF4d7C9qizgIHq

[9] https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/?fbclid=IwZXh0bgNhZW0CMTAAAR1k5om7iA33TJM5H2KjM1cYyXgYtRDYlXqX2ARcOXrDEOVwe-Ydm6Q3Inc_aem_AaGkwze-VkbbKrrb8Etm2kvp5S91w-l3bM0H67QIkbtuE0k0j_Fj422TAkwz3h-hJrp_tDmMg4ci8j8F3SXR9BcC

[10] https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/?fbclid=IwZXh0bgNhZW0CMTEAAR01PriLB7nKV-9W0UFrZlYJ7jgwZD8mdZoZNAfQcmnHwrGpzFKW3iG5ek4_aem_AaGu4ds0kaFbzmmRJAi2wrPzfDlquW99f7QVIPQey10KQMEtlJoaSYpIH8JuF-SKbTrNwuDAN4YEPYx8yoXJsIJ0K

[11] https://aka.ms/ThreatIntel-Russia

✓ **March 2023.** An analytical summary by the International Institute for Strategic Studies (IISS)[12], which focuses not only on assessing the efforts of Ukraine and Russia, but also on the long-term challenges facing Ukraine in case of a protracted conflict (for example, a problem of an improvised nature of many cyber protection solutions, an active regrouping of Russian cyber specialists, etc.). The author's general conclusion confirms a similar one from the Carnegie Endowment – Ukraine's experience maybe so unique that it cannot be adapted as a reliable strategy by other countries.

✓ **May 2023.** The US think tank Center for Strategic and International Studies (CSIS)[13] has presented a comprehensive study "Evolving Cyber Operations and Capabilities". The series of essays describes various aspects of cyber confrontation, including an importance of information sharing among allies, the need of public-private partnerships, but also notes caution in trying to copy the Ukrainian experience of resistance, as the aggressor has demonstrated significant incompetence that all other aggressors will avoid.

✓ **July 2023.** The US think tank Center for Strategic and International Studies (CSIS)[14] presented another research on the first year of the cyber warfare and pointed out a lack of reliable (verifiable) data that Russian cyber activity has reoriented or changed since February 2022 regarding the goals that were relevant to it in previous years. At the same time, although dynamics of attacks have increased, their severity and effectiveness have decreased.

✓ **September 2023.** Assessments of the UK National Cyber Force (NCF)[15] based on assessments of General Tom Copinger-Symes. They focus on a migration of Ukrainian data to cloud services abroad and a crucial role of intelligence sharing with private companies as a factor in effectively countering cyber offense.

✓ **December 2023.** A comprehensive study by Chatham House "Russian Cyber and Information Warfare in Practice[16]. The lessons learned emphasize an importance of Ukraine's flexible legislation (in particular, for the rapid procurement or use of research technologies), rapid relocation of data to clouds and creation of a cyber proxy (IT army). Like several other researches, Chatham House experts point out that Ukraine's better understanding of Russian strategic culture, warfare doctrines and Russian mentality is a factor of resistance. They also note a limited impact of cyber operations in case of a kinetic conflict – under such circumstances, cyber operations are mostly aimed at intelligence gathering or psychological warfare rather than destruction.

[12] https://www.iiss.org/research-paper//2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences?fbclid=IwZXh0bgN-hZW0CMTEAAR2PylrEkD6mzK3L7B3I9KOyYcaWmUtYMLtHe3IGQPf5b3-MiblRXQZRH_k_aem_AaHS-xvk2JzNQAH0zgTuaPrVPDA7EnkHRJH4kM-fKfnIoXWa0CPBPMHkJocJ2T3z972ogQQ2CORN4rtoJHRa15Jb0

[13] https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-05/230518_Lewis_Evolving_Cyber_2.pdf?VersionId=CG3NiGS8QK8RZt.1xZAd-JSBpVFxEAamB

[14] https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war?fbclid=IwZXh0bgNhZW0CMTEAAR1sdQ1_OeCPeBx2gxCv_3fRx-erjLR-q09bHNtYQcXlnywaV95blWEkF1QA_aem_AaGOUSg-tV1hyKQ30O5dQS7mNQ3mdBN6mlBa_vMkoLOjGLq33rKtQDw7ZgeQteSb4r3kSTvIqcRkf1HLgwhBeAs-

[15] https://therecord.media/uk-hunt-forward-operations-lt-gen-tom-copinger-symes?fbclid=IwZXh0bgNhZW0CMTEAAR0Ke10Vv93yMK_-sho4RjsGVU6mHE6MzJVgTpnxQfUACddZL6owaMkpU_M_aem_AaH0uuiyhUn4Wk0LqUroRztyt6iCZ_jeUVPLwTPXb_hJgg_mlKflXeJx_WReLFJA71na6yHB2UtY-p867qE82q3Q

[16] https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/05-lessons-observed

✓ **February 2024.** Another analysis of the situation and lessons from Carnegie Endowment For International Peace[17]. The author of the research notes that Ukriane's cyber resilience was largely boosted by Russia's constant cyber-attacks, which began in 2014 and have effectively "strengthened" the Ukrainian cybersecurity system, which was ready for the enemy activity.

There are still not too many similar reflections on the lessons of cyber warfare from Ukrainian experts (at least in terms of public assessments, which are not presented at various events). Among the most notable are:

✓ **May-July 2022.** Experts at the National Institute for Strategic Studies[18, 19, 20] have made several reviews of the first lessons of cyber warfare. However, these are mostly summaries of data available at the time, not their own conclusions and assessments.

✓ **January 2023.** Research[21] by a team of the Civil Association "Economic Security Council of Ukraine" regarding a connection among cyberattacks, kinetic attacks and Moscow's propaganda actions. Although the research was not directly targeted at studying the lessons of cyber warfare, authors draw some conclusions: no "new" types of cyberattacks – the enemy uses known tools, cyberattacks are often coordinated with other domains of confrontation, there is no reason to believe that an intensity of cyberattacks will decrease.

✓ **March 2023.** Research of the State Service of Special Communications and Information Protection of Ukraine on lessons learned in 2022[22]. The document focuses on changes in a focus of Russian government-backed attackers' attention that took place in both halves of 2022. In particular, in the second half of the research, the State Service of Special Communications and Information Protection of Ukraine recorded a shift in the focus of Russian hackers from media and telecommunications industries, which were among the main targets at the beginning of the warfare, to the energy system, which has also become one of the main targets of Russian missile attacks since October 2023. In addition, the targets of Russian hackers have also changed: from many destructive attacks to espionage and data theft.

✓ **February 2024**. For the 2024 Kyiv International Cyber Resilience Forum, a group of authors prepared a review "Decades in Trenches of Cyber Warfare: The Story of Ukrainian Resilience"[23], which analyses an evolution of Ukraine's cybersecurity landscape since the beginning of 2013. A separate section of the document is devoted to the cyber confrontation of 2022-2023 and points to a change in the tactics of Russian attackers between 2013-2021 and since the beginning of 2022. The first period was characterized by a variety of techniques, tactics and procedures, but during the active phase, the enemy focused on the most proven and effective approaches.

[17] https://carnegieendowment.org/research/2024/02/russias-countervalue-cyber-approach-utility-or-futility?lang=en

[18] https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/svitove-vidlunnya-rosiysko-ukrayinskoho-kiberprotystoyannya

[19] https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/doslidzhennya-shchodo-bezpeky-danykh-vid-verizon-holovni-vysnovky

[20] https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/kiberskladnyk-rosiysko-ukrayinskoyi-viyny-uroky-ta-otsinky

[21] https://reb.org.ua/storage/164/zagalnii-analiz-vimiriv-rosiiskoi-viiskovoi-agresi....pdf

[22] https://cip.gov.ua/services/cm/api/attachment/download?id=53466

[23] https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf

These, as well as some other attempts to summarize the lessons of the cyber confrontation between Russia and Ukraine that were not part of this review, can be summarized as follows:

✓ **Russia failed to achieve its strategic goals through cyberattacks.** Experts mostly agree that Russia failed to achieve its goals in cyberspace. This has led to the aggressor being forced to more actively use classical kinetic attacks against targets that it had previously planned to hit with cyber means. At the same time, there is a debate among various experts about a relevance of the goals and, perhaps, the real goals were achieved within the objectives set by initiators of cyberattacks (however, these objectives were much narrower than expected by external observers). Some experts believe that actions of Russian state hackers are overly rationalized, while their motives and actions are more driven by international imperatives of organizations in which they operate[24];

✓ **critical infrastructure (CI) is still a desirable target for the aggressor, but the ability to influence is less than expected.** There have been only the few really successful attacks against the CI during this period: a cyberattack on the satellite communications provider VIASAT (KA-SAT satellite)[25], an attempted cyberattack in April 2022 on Ukrainian energy facilities using Industroyer2 and CADDYWIPER[26] and a successful cyberattack against Kyivstar in December 2023. Such achievements are rather dubious from a point of view of a "grand cyber strategy", if Russia really has one;

✓ **during the time of military aggression, cyber espionage becomes even more important.** The aggressor's ability to carry out a successful cyber sabotage is severely limited if an effective cyber protection system is in place. The warfare in Ukraine has shown that the only cyber operations that remain effective in this period are cyber espionage or support for information operations;

✓ **a security of data centers is as important as their cybersecurity.** Although most threats to data center security are considered in terms of cybersecurity, physical protection has also important. American experts aptly point out that data centers are rarely designed with a possibility of a missile strike against them, but this probability is not equal to zero[27];

✓ **a rapid increase in a number of cyberattacks was observed prior to the invasion.** Cyberattacks in January and February 2022 against state registers and several websites were at a higher scale[28] than subsequent cyber activity. Experts[29] say that after the massive cyberattacks of the first 3-7 days of the aggression, there was a noticeable pause in cyber activity. It is unlikely that such high peak rates in other cases can be reliably interpreted as preparations for a military invasion, but it is not impossible;

[24] https://www.svoboda.org/a/tseli-stanut-masshtabnee-kto-pobezhdaet-v-kibervoyne-rossii-i-ukrainy-/32741896.html?fbclid=IwZXh0bgN-hZW0CMTEAAR11aa_oHy4BzZcwoRd1paxHpASJZ5QjYIeh1Ww_p23vEmlJN3aDpGrttjM_aem_AZsNfh-ScN1DyFNlUDiph906bftP51voMUVS-naqeFtqTuUbCDi0iT0ulN_ZD3Sw-cE0RvvJsEqYf3xrXuHtQmiEC

[25] https://dev.ua/news/hakeri-zlamali-suputnik

[26] https://cert.gov.ua/article/39518

[27] https://www.youtube.com/watch?v=ZMIkA85a5PY

[28] https://cutt.ly/nGKYY4s

[29] No Name Podcast with the Grugq - https://www.youtube.com/watch?v=zb_W_hRkX4o , 26.0.2022

✓ **the nature of cyber security units does not change much in terms of functionality – only the intensity of work increases.** Although it was expected that martial law and large-scale cyber confrontation would change tasks and functions of cyber security units, the most noticeable change was an increase in the intensity of their work;

✓ **cooperation between the state and private sector with individual citizens is critical but needs to be improved.** Rapid assistance to Ukraine from well-known cybersecurity companies was critical in the first months of the warfare. They provided intelligence on cyber threats (having their own extensive network of sensors that collect telemetry), assisted to hunt for cyber threats, and an expert support was needed to quickly restore a functioning of affected systems[30]. Direct assistance by individuals (without military status) to state structures was also important. However, such cooperation was unsystematic and poorly institutionalized;

✓ **the aggressor used no new tactics, techniques and procedures (TTPs).** Researches have not noted any noticeable change in the structure of cyberattacks, although they point to an emergence of a number of new malicious groups and malware (Ransomware[31] and Wiper[32]) in a period before the aggression and in the first months after it. Among few changes in hackers' tactics are the following: instead of long-term attempts to attack direct targets, they began to concentrate on peripheral targets, such as firewalls, routers and email servers;

✓ **during military operations, the aggressor does not conceal its involvement in destructive cyber activity.** While before the warfare, Russian hackers tried to hide the infrastructure from which they conducted cyberattacks, with a start of the aggression, cyberattacks were almost openly launched from Russian territory. Therefore, in a context of the full-scale military conflict, a problem of attributing cyberattacks almost disappears from the agenda;

✓ **ensuring secure communications (between the state administration and the Armed Forces).** Russians attempted to disrupt this communication, apparently hoping to increase chaos and reduce a controllability of the Ukrainian Armed Forces. For this purpose, the VIASAT satellite communications system (KA-SAT[33]) was attacked, which was actively used by the Ukrainian Armed Forces. Duplication of communication channels and creation of alternatives is important to maintain control of the situation in the most difficult first weeks of the aggression;

✓ **when planning offensive cyber operations, it is important to balance a right intensity among factors such as "intensity-speed-control".** The aggressor's cyber activity has shown that it has not been able to find an optimal balance among three factors that directly affect the results of cyber activity: *speed* (how quickly attacks can be carried out), *intensity* (how

[30] https://www.infosecurity-magazine.com/news/nsa-6-takeaways-war-ukraine/?fbclid=IwAR0kYnGtvRe9Naypct_i7qpmH5LKHaY16IsHv2-8bVUwsBYjBy5u8OzVVVo

[31] Ransomware – both the name of the type of virus and the name of the type of malicious activity. With the aid of malware, all information of the attacked object is encrypted and a ransom is demanded for its decryption (ransom).

[32] Wiper - malware that aims to wipe a hard drive of a victim machine, i.e. destroys data using various methods. Often imitates the activities of Ransomware.

[33] https://dev.ua/news/hakeri-zlamali-suputnik

powerful and prolonged they will be), and *control* (how well they are managed and coordinated). In fact, anyone using cyber offensive methods has to balance these factors, focusing on only two of the three at a time[34];

✓ **the mass movement of cyber volunteers is important but needs to be properly coordinated.** While activities of mass movements of cyber volunteers are important, a nature of their attack techniques (mainly DDoS attacks) raises a question about an importance of their effective coordination with those conducting more sophisticated cyber operations. Experts point out[35], that DDoS attacks against the aggressor state's websites in a context of large-scale military aggression have more of a psychological relief effect for large groups of people than they can actually change the aggressor's behavior. At the same time, uncoordinated attacks could interfere with other influence operations of pro-Ukrainian cyber specialists. Another conclusion from the large-scale activities of cyber volunteers is that their active involvement in cyber confrontation continues to blur lines between civilian and military participants, and thus the issue of responsibility (legal) for certain actions[36].

In addition, experts are still discussing an extent to which the experience of the Russian-Ukrainian cyber warfare can be extrapolated to other similar situations (for example, the potential escalation around Taiwan) and whether these lessons can be learned by other countries to better prepare for possible aggression. There is a growing idea that possibilities of such an application outside of Ukraine are rather low, and that Ukrainian case is unique in many ways. The physical size of Ukraine, specifics of the Ukrainian-Russian relations since 2012, and Russia's underestimation of Ukraine prior to the invasion are all factors that are difficult to replicate in another region. Experts rightly point out that it is unlikely that another aggressor will underestimate its opponent to repeat Russia's mistakes.

The only thing almost all researches agree on are common lessons that can and should be applied by all are the following:

☞ strengthening a partnership between the public and private sector;

☞ cyber intelligence sharing among partner countries;

☞ greater focus on financing and building protective systems (which have proven to be effective);

☞ a permanent strategy to develop "resilience" instead of "rigid" protection;

☞ understanding how to interact with potential cyber attackers.

[34] https://www.youtube.com/watch?v=olgf_gFhuBc

[35] https://youtu.be/olgf_gFhuBc?t=590

[36] https://warontherocks.com/2022/12/disentangling-the-digital-battlefield-how-the-internet-has-changed-war/

METHODOLOGY AND DESIGN OF THE RESEARCH

The main basis of the research was a survey of experts from state agencies, critical infrastructure facilities and the private sector by questionnaire. With an assistance of the National Security and Defense Council of Ukraine, questionaries were sent to respondents representing main entities of the national cybersecurity system, central and regional authorities, private companies and critical infrastructure facilities.

The questionnaire is divided intro three semantic blocks:

The purpose of the first block of questions was to retrospectively understand what expectations of cybersecurity entities were, what challenges they were preparing for and how they perceived a level of cyber readiness of the state.

The second block was to provide a broader understanding of what happened after the 24th of February 2022, how well the events of this period met expectations and preparations, and how well actions of various entities were coordinated.

The third and fourth blocks are an assessment of the most effective measures taken and what measures worked, and what did not.

In total, 287 participant questionnaires were received, including:

☑ 108 – state agencies that are not the main subject to cybersecurity;
☑ 119 – experts of one of the main cybersecurity entities;
☑ 44 – CI facilities;
☑ 5 – private companies and individual independent experts;
☑ 3 – local authorities.

In general, participants self-identified as:

☑ 163 – specialists;
☑ 43 – heads of independent units within departments (heads of divisions);
☑ 17 – heads of departments;
☑ 15 – deputy heads of independent units within department;
☑ 12 – deputy heads of organizations;
☑ 2 – heads of organizations;
☑ 41 – other variants (chief specialists, specialists, employees of non-core departments, etc.).

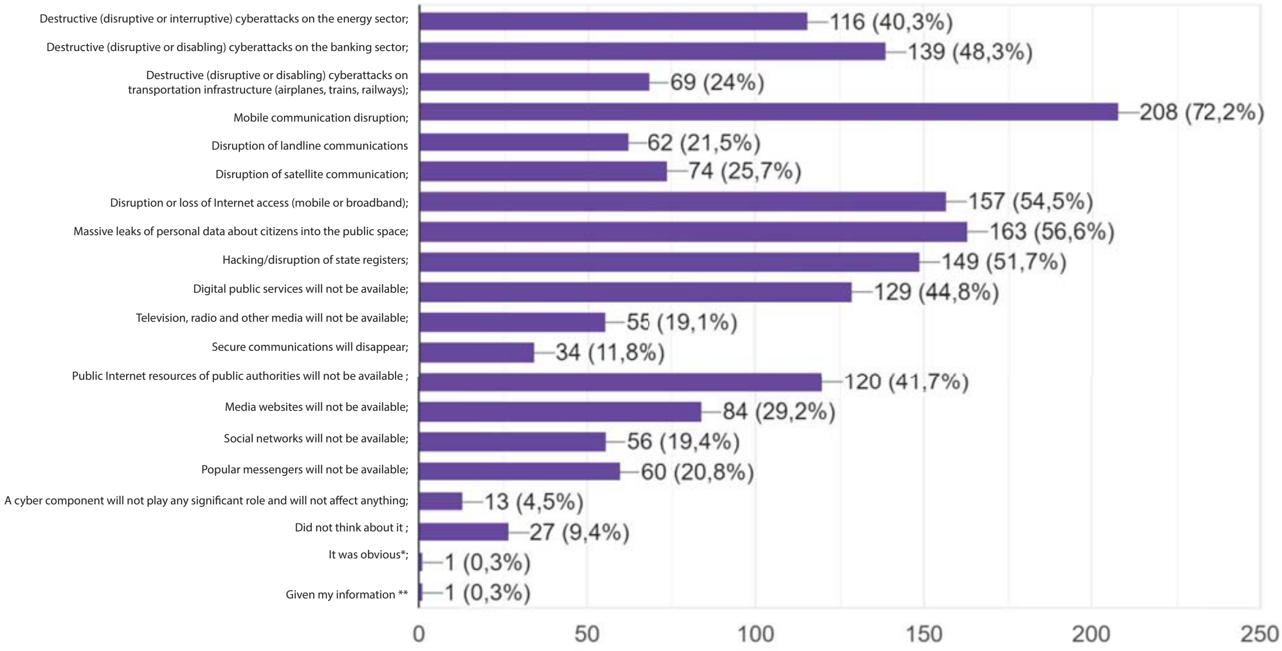
There are 67% of participants, who started working for their organization before the 24th of February 2022, so they can compare organizational expectations. Almost all participants are specialists in cybersecurity or related activities.

KEY CONCLUSIONS

I. Expectations appeared to be worse than reality

From the list of answers prepared in advance by experts, respondents were asked to select a number of typical expectations of what might happen as a result of cyberattacks.

1.1. Looking back at your expectations before the 24th of February 2022, would you say that you thought that cyberattacks would result in...: (please select any number of answers) – 288 answers:



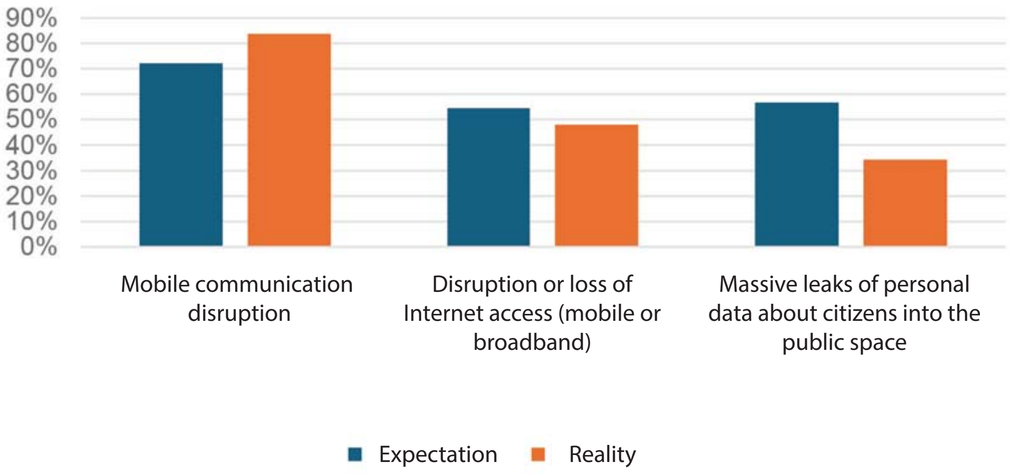
* It was obvious that the cyber component would not play an independent role in all processes, but there would be a hybrid implementation of each of the listed scenarios, taking into account "military necessity", and "barbaric attacks" were expected, which would have no meaning - 1 (0.3%);

** Given my information and knowledge at the time, I expected what was possible as a result of cyberattacks: Destructive (disruption or cessation of functioning); cyberattacks on the Energy sector: partial or localized power outages; Banking sector: interruptions in the operation of online banking, ATMs, payment systems; Transportation infrastructure: flight delays, disruption of control systems; Disruption: Mobile communications: localized disruptions; Fixed-line communications: localized disruptions; Satellite communications: localized disruptions; Internet access: localized disruptions; Massive leaks of personal data about citizens: likely, but not widespread; Hacking/disruption of state registries: likely, but not widespread; Inaccessibility: Digital public services: partial; Television, radio and other media, local disruptions; Disappearance of Special Communication: likely; Public Internet resources of public authorities: likely; Internet pages, media: likely; Social networks: likely; Popular messengers: likely; It is important to note that I did not expect this: Complete and large-scale neutralization of all the above systems. The absence of a cyber component in this warfare. In my opinion, cyber warfare would play a significant role in the conflict, but its impact would not be total. It should be noted that the real consequences of cyberattacks could differ from my expectations - 1 (0.3%).

The absolute record-breaker was an expectation that there would be destructive attacks (i.e. direct disruption or termination of functioning) of mobile communications as such (72%), massive personal data leaks (56.6%), and disruption or disappearance of mobile/broadband internet access (54.4%). One respondent explicitly stated that "since most state and private sector organizations do not have an appropriate protection (even at the basic and medium level), I expected a complete collapse of the communication infrastructure, as well as a suspension/slowdown of all businesses and state agencies".

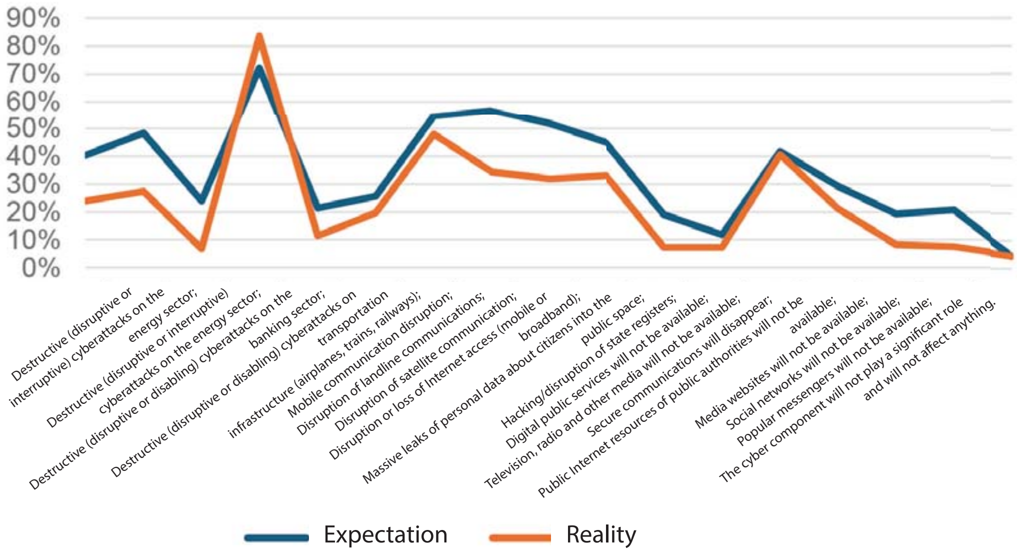
In fact, these general expectations were partially met. Answering the questions "Based on your experience and knowledge, from today's perspective, which of the following has come true since the 24th of February 2022 due to cyberattacks", respondents confirmed that these expectations were met.

The most expected consequences of cyberattacks and the reality of their realization



At the same time, a more general framework of expectations of cyber threats is also interesting, primarily in terms of comparison with the current situation (or rather how it was perceived after the 24th of February 2022).

Comparative Dynamics of Expectations vs. Reality Regarding the Consequences of Russian Cyber Activity:



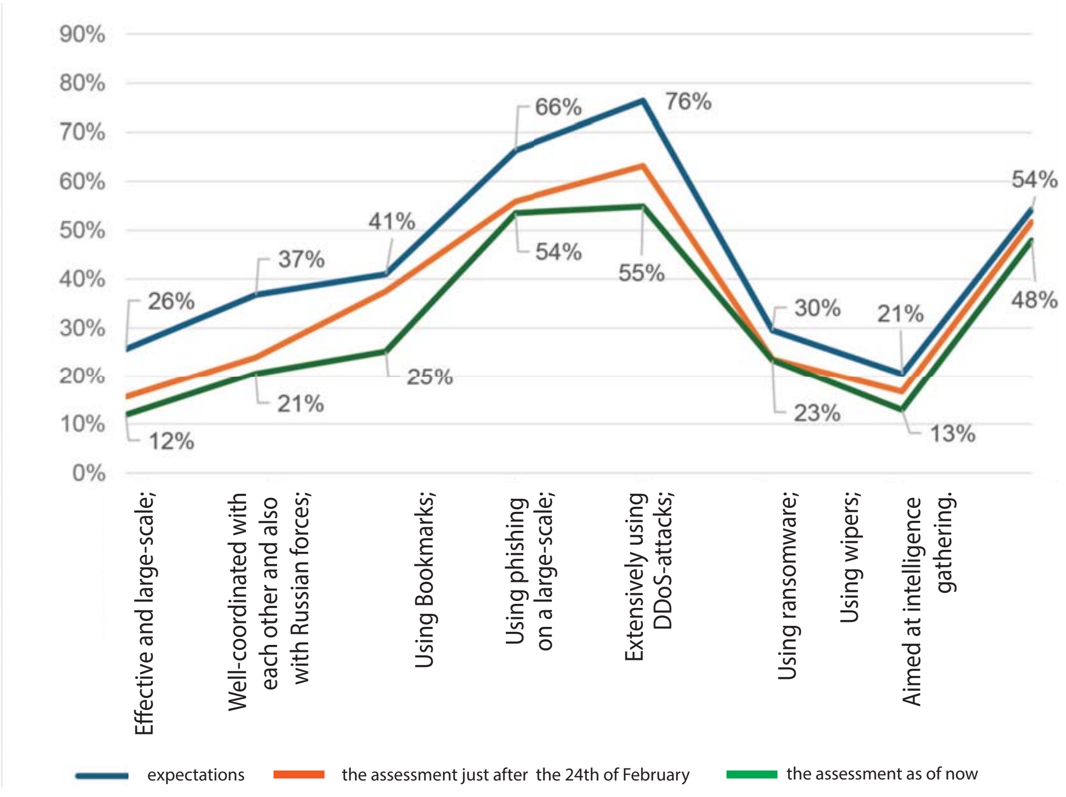
In general, expectations were much more catastrophic than the actual outcome. Some positions (for example, a threat to an availability of television, radio, social networks, messengers) were overestimated by almost 3 times.

It is also interesting to note that almost 50% of respondents highly assessed a likelihood of a disruptive attack on the energy, banking and transport sectors, but the actual threat assessment reflects a significantly lower threat to these sectors than could be expected (for the transport sector, the actual threat situation was 3 times lower than expected).

II. Russian capability regarding methods and coordinated attacks was overestimated

Similarly to the previous observation, we can note very high expectations of respondents regarding methods that Russians will use and effectiveness of their use.

Expectations and reality regarding Russian cyberattacks:

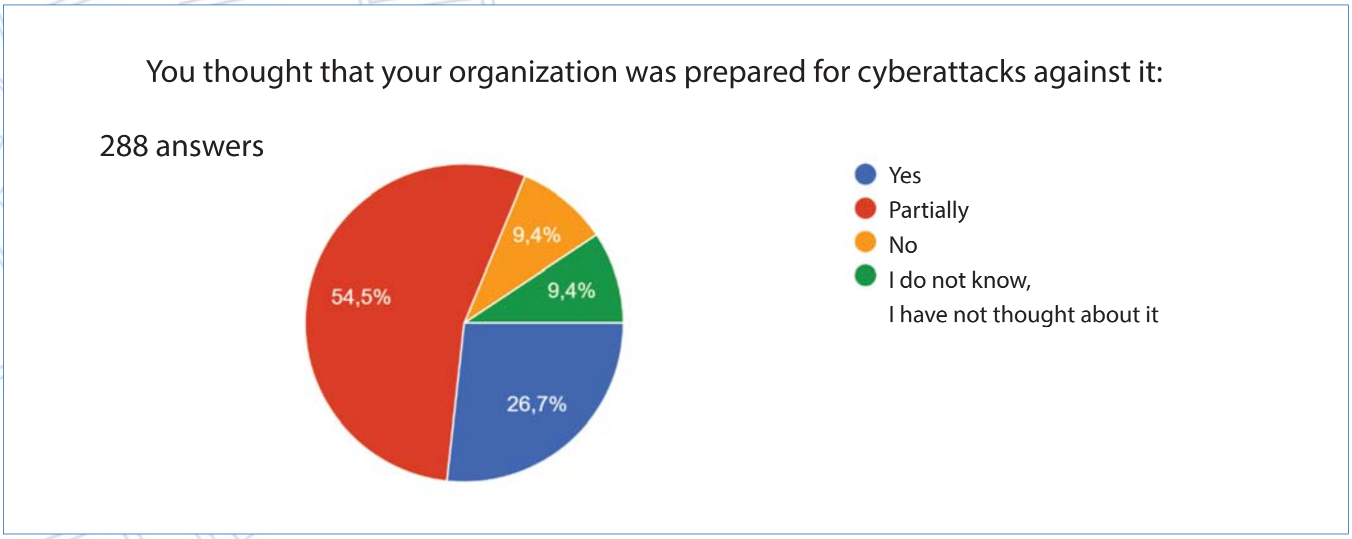


Some figures are particularly illustrative. For example, expectations about an overall effectiveness and scale of Russian cyber activity differ by almost 2 times between what was expected and what actually happened. There are 26% of respondents expected Russian cyberattacks to be large-scale and well-coordinated. This estimate is significantly higher than the actual figure after the 24th of February 2022, which is 12%. There was also great concern about a possibility of bookmarking, with 41% of respondents believing that this threat was real. In fact, after the 24th of February 2022, only 25% of respondents said that this threat was relevant. The smallest discrepancy is in the issue of intelligence gathering (54% of expectations vs. 48% of the actual situation), the usage of ransomware (30% vs. 23%) and phishing (66% expected such activity, only 54% indicate that this threat has come true).

The survey did not seek to identify reasons why respondents assessed these threats in this way. At the same time, it can be assumed that this overestimation was based on media publications, assessments of Russian cyber capabilities based on the previous experience of Ukrainian cyber experts (cyberattack against Prykarpattyaoblenergo, NotPetya, etc.).

III. Organizations doubted their readiness to cyberattacks, but were generally prepared

There are 54% of respondents indicated that by the 24th of February 2022, they assessed their organizations' preparedness for cyberattacks as "partial" (only 26.7 % clearly stated that they were prepared). This is correlative to other data on confidence that "State sector organizations are well protected against cyberattacks". There are 59% of respondents indicated partial security (only 10% answered "Yes" to this question).



You thought that your organization was prepared for cyberattacks against it:

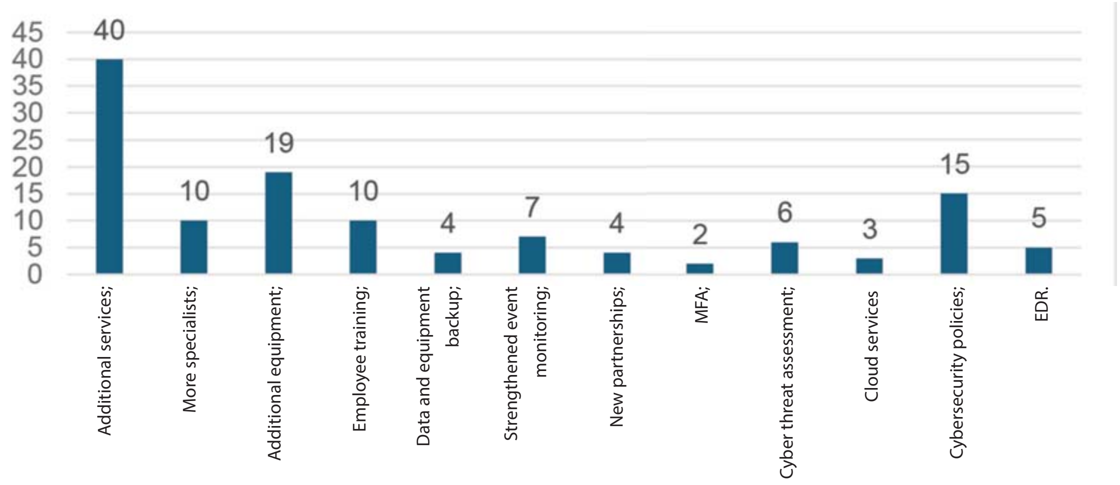
288 answers

This data is supported by a similar question about the actual cybersecurity situation in organizations after the 24th of February – 63% answered "Yes" to the question "Assessing cyber activity after the 24th of February 2022, would you say that your organization was prepared for cyberattacks against it?". One of the factors of such readiness was probably the cyberattacks on the 13th and14th of January 2022 (the first phase of cyber aggression). There are 51.2% of respondents indicated that their organizations had taken these attacks into account and strengthened cybersecurity measures, while 27.2% had not taken any additional measures. When assessing whether these measures assisted to counteract cyberattacks after the 24th of February 2022, 37.6% of respondents noted the effectiveness of the measures taken. Some organizations explicitly stated that additional employee training was conducted, infrastructure was completely rebuilt, and additional resources were deployed to prepare for cyberattacks. In particular, the respondents (77 organizations in total) mentioned the following additional measures:

- ✓ connected additional cybersecurity services and strengthened monitoring measures;
- ✓ attracted more specialists;
- ✓ connected additional equipment;
- ✓ improved the level of cyber hygiene and provided intensive training for employees;
- ✓ implemented the Active Directory technology;
- ✓ ensured backup of critical information and systems;
- ✓ deployed the Cisco Umbrella system;
- ✓ deployed the FortiMail email gateway, etc.

In general, these steps can be summarized in 12 key categories. Their analysis suggests that a typical response of organizations to cyberattacks was to connect to additional cybersecurity services, purchase additional equipment, and implement/change cybersecurity policies in their organization. Additional training of employees (both those responsible for cybersecurity and their organization as a whole), additional specialists, and increased threat monitoring were also often carried out.

Measures taken after cyberattacks on the 13th and 14th of January 2022:



It should be noted that 36.6% of all respondents confirmed that additional measures were taken but did not have a significant impact on events after the 24th of February 2022.

IV. Knowledge of own capabilities and poor understanding of other organizations

The overwhelming majority of respondents (81.9%) were sure that they knew who to contact in case of a cyberattack against their organizations (only 8.3% answered "No" to this question). This figure was confirmed in the actual situation assessment block – 91.3% clearly knew who they could contact in case of a cyberattack against them.

However, their knowledge of a possible course of actions of other entities (and thus their general awareness of activities of other cybersecurity entities) was rather weak: only 36.8% answered affirmatively to the question "Do you know how other organizations would react and act in case of cyberattacks against them?". Interestingly, almost 25% of respondents answered, "I do not know, I have not thought about it". This may indicate that cybersecurity professionals are not aware of an interdependent nature of cyber threats and that the actions of other entities (and threats to them) may be closely related to security of their own organizations.

The same 25% said that they did not follow or think about how other cybersecurity entities respond to cyberattacks. At the same time, only 10% answered "Yes" to the question "Given an increased cyber activity after the 24th of February 2022, would you say that other organizations responded to cyberattacks exactly as you had predicted/expected?" – 58% said "More likely yes than no".

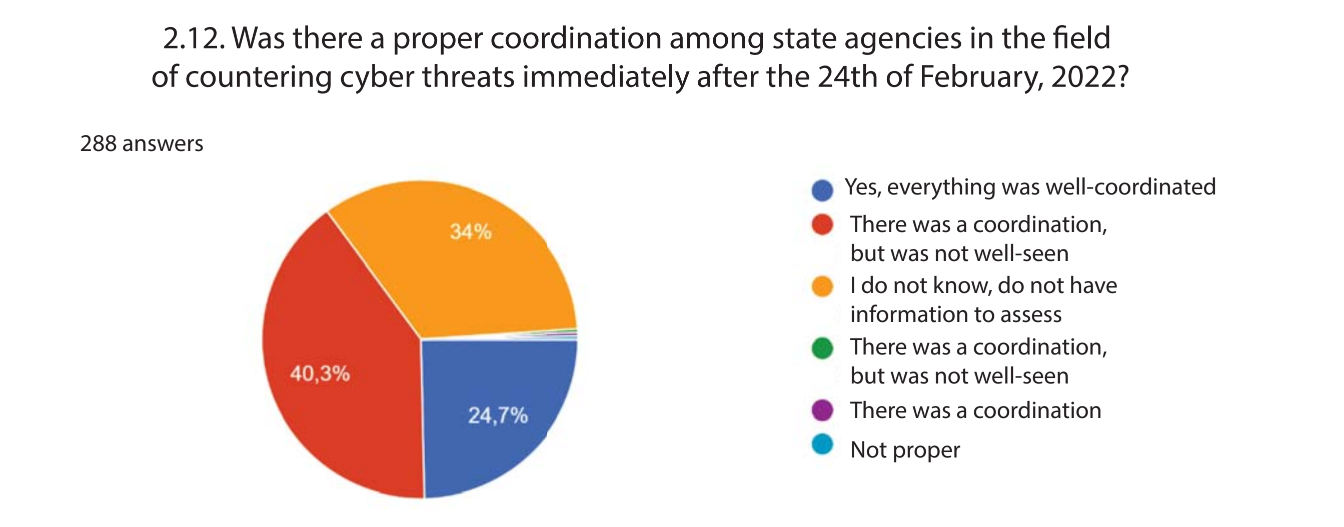
V. Effectiveness of coordination is assessed positively and there is a tendency for improvement

There are 12.5% of respondents (36 people) indicated that they personally participated in various tabletop exercises (e.g., National Cyber Readiness 2021, which was supported by the NCCC). Almost 18.1% of respondents said that representatives of their organizations had participated. However, 37.3% of respondents said they were not even aware of the existence of such exercises. This may indicate the need to strengthen an information campaign to engage various entities in this type of activity.

It is difficult to assess the effectives of such exercises in terms of practicing real coordination measures. However, 1.8% of respondents (which corresponds to a number of those who participated) stressed that this experience was useful for responding to hostile cyber activity after the 24th of February 2022. Another 9.8% of respondents noted the usefulness of the exercises but admitted that they did not act in accordance with the interaction protocols that were the focus of those exercises.

Although one respondent noted that he "expected more coordinated activities of the main entities", respondents generally gave a positive assessment of the state's coordination efforts in the field of cybersecurity immediately after the 24th of February 2022. There are 24.7% of respondents explicitly stated that coordination was at a proper level, and 40.3% were aware that it was taking place, although not very noticeably.

The respondents clearly indicate a positive trend in coordination practices – 50.7% say that they have improved significantly over the past 2 years, while 22% emphasize that they have not become worse ("they exist, but at the same level"). Although the questionnaire did not contain



2.12. Was there a proper coordination among state agencies in the field of countering cyber threats immediately after the 24th of February, 2022?

288 answers

open-ended questions that would indicate the reasons for the improvement, it can be assumed that this is due to adoption of several coordination tools (e.g. the Procedure for Interaction of Cybersecurity Entities in Response to Cyber Incidents/Cyberattacks) or an introduction of continuous exercises (trainings, tabletop exercises, etc.).

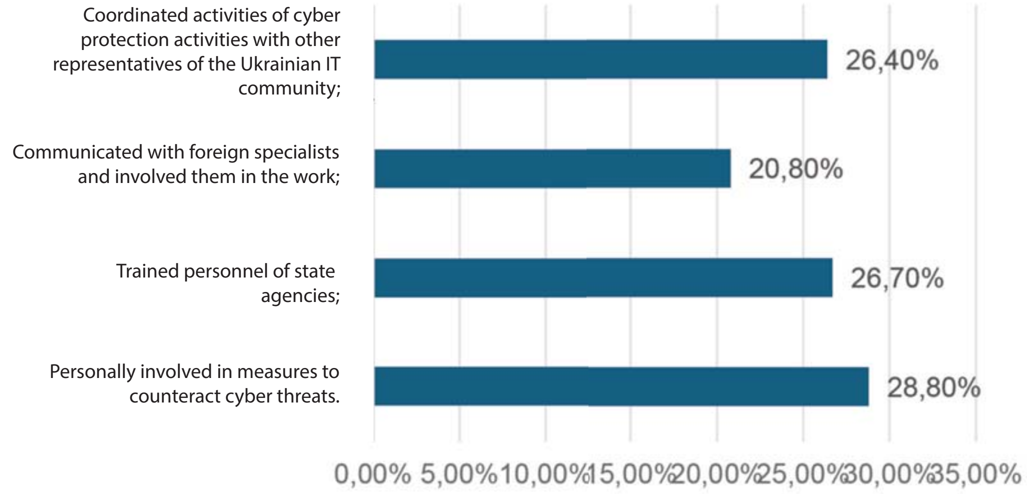
VI. Specialists of private sector were important in cyber resistance, despite the fact their influence on the situation was not always visible

While most international studies point to the exceptional role of the private sector in effectively countering Russian cyber aggression, survey respondents (49.7%) indicated that they had no information on this issue and therefore had not encountered private sector experts in a context of cyber activity after the 24th of February 2022. This is partially confirmed by the answers of 54.9% of respondents who do not have accurate information on the dynamics and forms of involvement of Ukrainian cyber experts from the non-governmental sector in the first months of the full-scale invasion and at the time of the survey. Such high rates of ignorance do not indicate a lack of private sector efforts, but rather a non-public nature of assistance, and probably its specific nature, when the assistance was provided to a relatively small number of key organizations (the main entities of the national cybersecurity system) and was multiplicative. Interestingly, 39.2% of all respondents believe that the large-scale involvement of cyber experts from the private sector has been a factor that has assisted Ukraine to be effective in countering cyber aggression.

There are 17.4% of respondents believe that private sector experts have been quickly and effectively involved in the country's cyber protection. Respondents divided forms of involvement into 4 formats in almost equal proportions.

There are 14,7% of respondents, who believe that the dynamics of involvement of Ukrainian cyber experts from the non-governmental sector has not decreased, but has increased. This 14.7% includes the answers "Involvement has increased in the same forms" and "Involvement has increased, but the form of assistance has changed". Another 8% of respondents believe that the level and forms of engagement have not changed, but 17.4$ emphasize that engagement has decreased.

Format for engaging private sector experts:



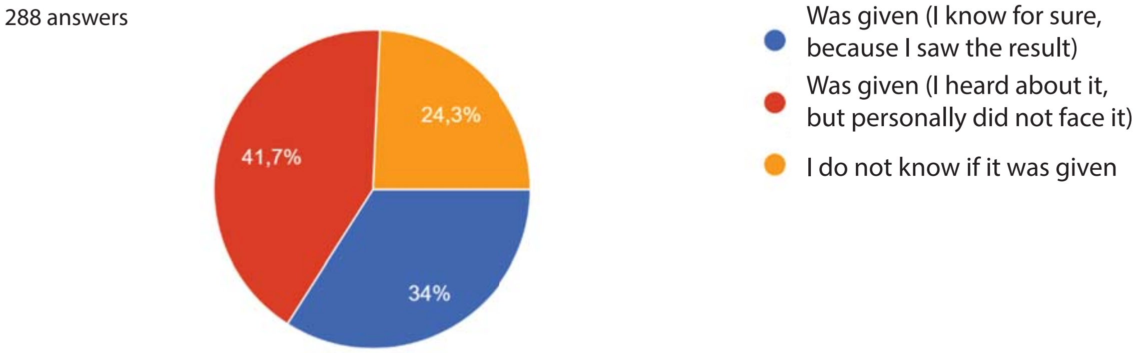
Assessing the coordination of private experts with state agencies, almost 14% of respondents believe that private and state cyber experts coordinated effectively with each other, while 16% believe that private sector cyber experts acted mostly independently (though effectively).

VII. International partners and assistance

International assistance is another factor that international experts point to as an important factor in Ukraine's cyber resistance. Respondents' assessments of this matter are more positive than in the case of the private sector. Overall, 75.7% of respondents either received such assistance after the 24th of February 2022 or heard that such assistance was provided.

Interestingly, 35.1% of respondents noted an importance of international technical assistance in preparing Ukraine to counteract cyber aggression after the 24th of February 2022. Another 42.7%

2.15. Assistance from international partners (in the field of cybersecurity) immediately after the 24th of February, 2022



of respondents emphasize a role of such assistance (new technologies or equipment) after the 24th of February 2022. At the same time, 23.6% of respondents point to the lack of clear procedures for seeking international cybersecurity assistance in an emergency.

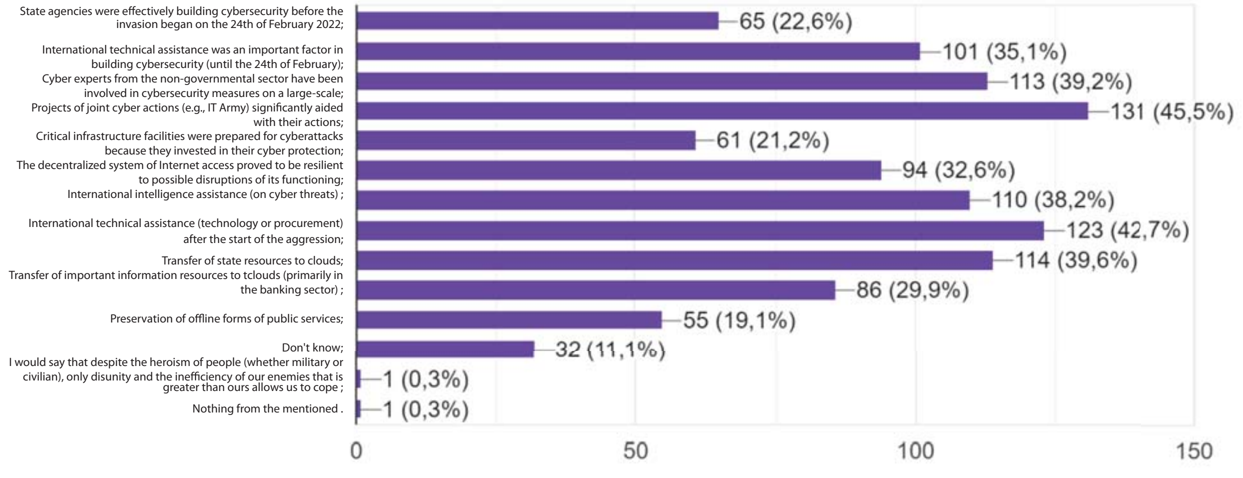
VIII. Joint action projects, international assistance and private sector experts are key elements of effective countering cyber aggression

The authors of the research prepared a list of statements for the respondents to identify key components that, in the respondents' opinion, took place and assisted Ukraine to be effective in countering cyber aggression. Most experts ranked joint action projects (including the IT army) first as an example of activities that have significantly contributed to counteracting cyber aggression, with 45.5% of respondents agreeing with this statement. International technical assistance with procurement (42.7%) and transferring of state registers to clouds (39.6%) are in the second and the third place.

Interestingly, only 21.2% of respondents (one of the lowest figures in this block) agreed that critical infrastructure facilities were prepared for cyberattacks because they had invested in protection in advance. At the same time, 45.8% of respondents said that the critical infrastructure facilities had coped well with cyberattacks after the 24th of February 2022, while 27.8% believed that they had done so mediocrely.

The similarly low rate of approval was given to the statement that "The state agencies were effectively building cybersecurity before the invasion of the 24th of February 2022". Only 22.6% of respondents agreed with this statement. This is confirmed by the answers of respondents to the question "Do you think state agencies did enough before the 24th of February 2022 to ensure Ukraine's cybersecurity?" – 65.3% answered negatively, while only 17.4% of respondents agreed with this statement. In fact, general assessments of respondents are having a negative perception

3.1 Which of the following statements can you characterize as having taken place and assisted Ukraine to be effective in countering cyber aggression? (please select any number of answers) – 288 answers:



(rather insufficient) of the efforts made by the state in the field of cybersecurity by the 24th of February 2022. Interestedly, this result is weakly correlated with positive assessments of the effectiveness of countering hostile cyber activity, a quality of coordination, and an imbalance in expectations and reality of cyber threats (with a focus on a marked exaggeration of expectations of threats) faced by Ukraine. It can be assumed that a persistent negative assessment of all the efforts made is partly a result of traditional skepticism about the effectiveness of state actions in any field.

Among other important factors, respondents noted an importance of moving state information resources to clouds (39.6%), international assistance with cyber threat intelligence (38.2%), and a de facto decentralized system of Internet access that ensured its invulnerability to cyberattacks (32.6%).

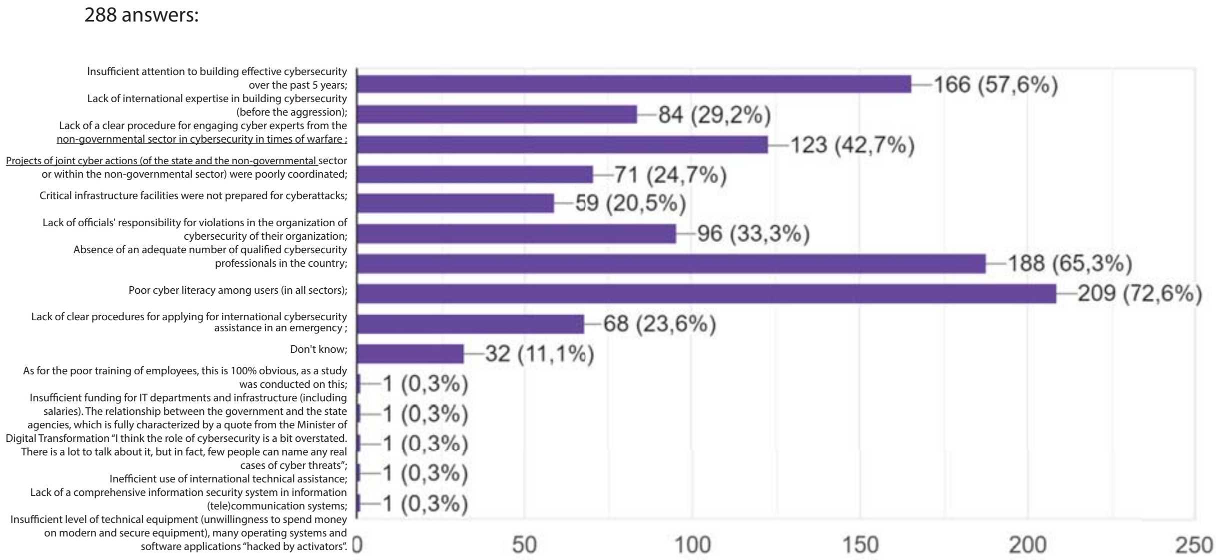
IX. Lack of cyber literacy, lack of specialists and insufficient efforts to build cybersecurity are key obstacles to cyber resistance

The respondents were asked to choose from a list of problems that prevented the state from being effective in countering cyber aggression.

In general, indicators on this issue were traditional. The key problem, which was agreed among 72.6% of respondents is that, that there was poor cyber literacy of all users, regardless of sector. Also, 65.3% of respondents noted a lack of sufficient cyber specialists. These two key issues were the focus of attention for many respondents. On the third place is sufficient attention to the development of effective cybersecurity over the past 5 years (57.6% of responses).

A lack of a clear procedure for engaging private sector cyber experts in cybersecurity during the warfare can also be considered as a major problem – 42.7% of respondents agreed with this statement.

4.1 Which of the following statements can you characterize as having taken place in Ukraine and preventing the state from being effective in countering cyber



The respondents were asked to choose from a list of problems that prevented the state from being effective in countering cyber aggression.

In general, indicators on this issue were traditional. The key problem, which was agreed among 72.6% of respondents is that, that there was poor cyber literacy of all users, regardless of sector. Also, 65.3% of respondents noted a lack of sufficient cyber specialists. These two key issues were the focus of attention for many respondents. On the third place is sufficient attention to the development of effective cybersecurity over the past 5 years (57.6% of responses).

A lack of a clear procedure for engaging private sector cyber experts in cybersecurity during the warfare can also be considered as a major problem – 42.7% of respondents agreed with this statement.

The three least critical problems are: a lack of preparedness of critical infrastructure facilities for cyberattacks (20.5%), a lack of clear procedures for seeking international technical assistance in an emergency (23.6%), and improper coordination of joint cyber action projects (between the state and the non-governmental sector or within the non-governmental sector itself) – only 24.7% of respondents agreed with this.

RECOMMENDATIONS

1. In general, the assessment of potential cyber threats was consistent with the actual results. At the same time, some of them were significantly overestimated by respondents. Such the overly catastrophic assessment may indicate that cybersecurity entities do not fully understand the real landscape of cyber threats in the country, which may strategically lead to inefficient use of funds for cybersecurity development, as well as improper preparation of cyber specialists for possible threat scenarios. It would be advisable to introduce at least one national document (possibly as part of the Cybersecurity State of the Art Review) that would provide generalized up-to-date assessments of the most important threats (a map of the cyber threat landscape), their gradation and potential danger of implementation. This would assist to optimize the efforts of cybersecurity agencies and focus them on the most important areas of counteraction.

2. More than 1/3 of organizations report that they have assessed the situation and implemented measures following the January 2022 attacks, and that this has had a positive impact on their preparedness for a new wave of cyberattacks. Thus, organizations that analyze cyber incidents, carry out the process of "Lessons learned" and act based on their results are indeed more prepared for new incidents. At the same time, it is not known whether all organizations have a methodology for conducting such the assessment and are trained to do so. It seems advisable to develop a standard procedure "After a cyber incident: how to evaluate your actions and learn lessons from the results", which would be approved by the NCCC and distributed among government organizations for practical use.

3. Continued operation of organizations in a crisis is critical in implementing the concept of resilience at the level of the national security system. Business continuity plans are one of the most important tools for such sustainable operations' preparation for cyber incidents. Based on the survey results, these documents should also include clear steps for organizations to engage additional cybersecurity services, equipment, specialists and staff training procedures.

4. Organizations (other than perhaps the main entities of the national cyber security system) have little awareness of possible responses of other organizations to cyber incidents. This is not a problem for isolated systems, but for supply chain attacks, it can create a situation where organizations at the same management level are dependent on how their partners or colleagues respond. This situation can be improved by increasing the number of tabletop exercises of various formats (including technical ones), as well as by introducing new forms of interaction among different entities. One of the options for the latter may be sectoral, thematic working groups under the NCCC of the National Security and Defense Council of Ukraine or under the response units of the main entities of the national cybersecurity system.

5. International studies point to a crucial importance of cooperation between state organizations and private sector cybersecurity experts. Almost half of the respondents indicated

that they were not aware of such facts or did not know how such specialists were involved after the 24th of February 2022. Apparently, such assistance was concentrated around a small number of organizations, but this raises a question of the need for boarder efforts by the state agencies to establish clearer procedures for such cooperation (and coordination, which only 14% of respondents consider effective), in particular to implement paragraph 8 of Strategic Objective C.4 of the Cybersecurity Strategy of Ukraine "to develop effective mechanisms for engaging private sector cybersecurity specialists in deterring and countering aggression against Ukraine in cyberspace". It would be advisable for the NCCC to intensify the actions of the responsible structures (the Cabinet of Ministers of Ukraine and the Security Service of Ukraine) to implement this paragraph.

6. The general perception of "sufficient state action in cyberspace" contrasts markedly with assessments of international experts and respondents' own assessments of the readiness of the state agencies to cyberattacks. Obviously, this problem is more cognitive than real and requires an informational and communicational solution. Currently, the NCCC prepares and spreads informational materials that summaries information about the state's actions in the field of cyberspace development (e.g. Cyber Digest, etc.), but these efforts are not enough. Perhaps the problem is that a "feeling of sufficient action" is highly dependent on a personal involvement of participants in a process that they would consider to be measures to strengthen it. Perhaps, the state needs to create a network of multi-purpose expert groups (similar to the principle of public-private partnerships' network in the US CISA) that would unite such specialists, give them an opportunity to cross path more often outside their job responsibilities, and interact on issues of improving a cybersecurity situation (with visible results).

7. There are 72,6% of respondents, who point to a problem of cyberliteracy/hyperawareness of users. Although this problem is already being addressed through national cyberliteracy campaigns, cybersecurity month, several non-governmental initiatives and numerous courses on the Diia portal. However, these efforts are still not enough. Ukraine obviously needs a truly systematic National Cybersecurity Program, as provided for in the current Cybersecurity Strategy of Ukraine, based on both national experience and international best practices (for example, through an implementation of the ENISA AR-in-the-box project). The next and the most important recommendation is to introduce mandatory cyber literacy tests for all civil servants and employees of Critical Infrastructure Facilities (first, state-owned, and in the future, all forms of ownership).