ECONOMIC SECURITY COUNCIL of UKRAINE

State Service of Special Communication and Information Protection of Ukraine

CYBER, ARTILLERY, PROPAGANDA

Comprehensive Analysis of Russian Warfare Dimensions

2022

CONTENT

The authors of the study have tracked the coordination of missile attacks on local governments and cyber attacks on community services, precise coordination of missile and cyber attacks on media and communication centers, and preparation and implementation of cyber attacks on institutions that help Ukraine (logistics, refugee support, and even cultural events), etc.

- Russian war against Ukraine has many dimensions: conventional, economic, cyber, informational, and cultural. Only understanding these dimensions' interaction allows for assessing the aggressor state's actions adequately.

- The world's first large-scale cyber war did not demonstrate new "types of weapons" in existing cyberspace. All attacks are carried out using previously known techniques. The attacks used by Russia have long been categorized and have straightforward solutions for counteraction.

- Cyberattacks are entirely consistent with Russia's overall military strategy. Moreover, cyber-attacks are often coordinated with other attacks: conventional attacks on the battlefield and information-psychological and propaganda operations. This effect was demonstrated in the autumn and winter of 2022, when, after a series of cyberattacks on the energy sector, Russia launched several waves of missile attacks on energy infrastructure. While simultaneously launching a propaganda campaign to shift responsibility for the consequences (power outages) to Ukrainian state authorities, local governments, or large Ukrainian businesses.

- Such coordination of attacks in different dimensions of aggression is widespread, although coordination is not an absolute constant rule.

- Doctrinally, Russia often considers cyber and information dimensions as a single "information confrontation" domain. This confrontation can include either pure information campaigns or something more complex. However, in any case, the goal

is information manipulation, to which all democratic regimes are naturally vulnerable.

- Cyber attacks, like conventional attacks of the Russian Federation, do not recognize any rules - infrastructure, humanitarian organizations, and private and state-owned companies are under attack. Russian hackers do not accept restrictions and do not recognize international borders, attacking different countries if they cooperate with Ukraine.

- There is no reason to believe that the intensity of cyber attacks will decrease. The only question is what they will focus on.

  — The study shows that it is necessary to adapt military doctrines to modern challenges, using the lessons of the Ukrainian-Russian war for forecasting and modeling tactics to effectively stand up against Russia and other authoritarian regimes.

  — Change legal approaches to the definition of aggression, significantly expanding the relevant legal interpretations;

  — Restrict authoritarian regimes' access to modern technologies by strengthening sanctions, including sanctions against the most critical sectors of the economy of such regimes.

The multidimensionality of Russian aggression manifested itself even before the full-scale invasion. Examples are the so-called "economic wars" and powerful hostile propaganda campaigns. But on February 24, 2022, the correlation between different types of attacks became systemic.

Russia practiced this tactic in previous armed conflicts (for example, during the aggression against Georgia). If it is not studied and effectively countered, this tactic will be used in the future against other countries. For example, suppose Russia has yet to receive a solid response for all its aggressive actions against Ukraine. If no hefty action is taken, it will return with even more daring attacks that will not be limited to Ukraine or our region alone.

The need to protect against multidimensional aggression creates a demand for:

- multidimensional information and multidimensional (not isolated) forecasts
- multidimensional strategies to counter attacks;
- multidimensional legal responsibility of the aggressor.

> Another critical issue is the need for complete economic isolation of the aggressor state. First of all, it is about restricting access to all modern technologies. After all, those are all used by Russia as a weapon.

Unfortunately, the international community lacks these components necessary for success. For that reason, most of the developments need to be sufficiently systematized. Therefore, it is essential to change all approaches urgently.

It is commonly believed that cyber-attacks are the weapon of the future. However, the war in Ukraine proved that this future is already here. Therefore, defense doctrines and international laws must adapt quickly.

The multidimensionality of warfare is a new security challenge (which could have been predicted but still needs to be adequately prepared for). There is no doubt that Russia is not the only threat to international security. Other authoritarian regimes will also conclude and use these approaches in the future.

Paradoxically, conventional attacks may eventually yield to cyber attacks in their negative consequences. Even today, in the example of Russian aggression, we can see hackers attack every object. However, in priority:

- state institutions (as decision-making centers responsible for maintaining stability within the country)
- civilian and energy infrastructure (because Russia is a terrorist who wants to increase the suffering of civilians without having successes on the battlefield),
- media and communications (these attacks strengthen Russian propaganda, a proven weapon of the Putin regime).

The main goal of Russian hackers has changed since the beginning of the war. Before the invasion and in the first month of the war, cyberattacks were aimed at the communication department, which was supposed to limit the functionality of the military and government in Ukraine. However, after the first defeat at the front, the Russian aggressor focused on inflicting maximum damage on the civilian population. This change of strategy can be traced in all dimensions of aggression. The attack on energy infrastructure is the best example. This attack was well thought out both in terms of timing and targets. During the cold snap, the first massive attacks on the energy infrastructure took place to put additional pressure on the civilian population, which adapts to inconveniences much worse than the military.

Therefore, the main task for Ukraine and our international partners is to identify all correlations in the Russian Federation's actions and develop a comprehensive strategy to counter these attacks.

INTERCONNECTIONS BETWEEN EVENTS OF DIFFERENT DIMENSIONS OF RUSSIAN AGGRESSION ○ *TIMEFRAME*

The intensification of large-scale cyberattacks preceded the conventional full-scale invasion.

On February 15, Russian hackers launched the most powerful DDoS attack in the history of Ukraine, which, among other things, was aimed at the financial sector (DDoS attack on 15 banking sites, sites with the gov.ua domain, as well as sites of the Ministry of Defense, the Armed Forces and the Ministry of Reintegration of the Temporarily Occupied Territories, which lasted about 5 hours). On February 23, before the Russian invasion of Ukraine, several government and banking websites were attacked again. According to the state-owned electricity transmission system operator Ukrenergo, the peak of cyber attacks against the energy sector occurred when the Ukrainian power grid was connected to the European ENTSO-E (i.e., on February 23-24). During some attacks on Ukrenergo, Russian hackers did not even try to hide their origin and used Russian IP addresses to scan the network of the state-owned energy operator.

> Thus, the cyberattacks were designed to increase the chaos of a conventional invasion, reduce the country's governability, and damage critical infrastructure.

FEBRUARY

February 24

A large-scale cyberattack disrupted satellite Internet access. Hackers disabled modems that communicate with Viasat's KA-SAT satellite, which provides Internet access to customers in Europe, including Ukraine.

February 24

On February 24, Russian troops launched a large-scale invasion of Ukraine, accompanied by rocket attacks on civilian and military targets.

With the beginning of the conventional full-scale invasion, information attacks also intensified[4]. In particular, until February 16, there were almost no information attacks. However, from February 17 to 23, there was a slight increase in such attacks. Starting on February 24, there was a peak of activity - 23 manipulative cases were recorded (which sowed panic, called for surrender, etc.). High activity of information attacks continued to be observed throughout March.

The hacker attack on the satellite Internet service began on February 24 between 05:00 and 09:00, just as Russian troops began shelling Ukrainian cities and entering the country.

Former U.S. Special Operations Command representative Pablo Breuer said the disconnection of the satellite Internet connection could complicate Ukraine's fight against Russian troops. *"If you are using modern intelligent systems, intelligent weapons, trying to perform combined arms maneuvers, you have to rely on these satellites,"* **Breuer said.**[5]

Subsequently, the United States, the United Kingdom, and the European Union accused Russia of a large-scale cyberattack on Ukraine on the eve of a full-scale invasion of Russian troops aimed at the satellite communications network.

According to experts, the main target was Ukraine's security forces, but the cyberattack also affected Ukrainian enterprises and individuals using Viasat equipment. In addition, the cyberattack also affected facilities outside Ukraine. Thus, in Germany, almost 6,000 wind turbines, the operation of which depended on Viasat routers, were disabled.[6]

PRESUMPTIONS

1. Powerful cyber attacks can precede large-scale conventional attacks.
2. Russia uses cyberattacks to weaken Ukraine and its ability to counter conventional aggression effectively.
3. The aggressor state does not care about the so-called "collateral damage"; Russia's cyberattacks in the war with Ukraine pose threats to civilians worldwide, especially in Europe.
4. Information attacks accompany conventional aggression and are significantly intensified simultaneously with the increase in the intensity of hostilities.

MARCH

March 1

DesertBlade malware was launched against Ukrainian TV companies.[7] As a result, Kyiv's media company faced destructive attacks and data theft.[8]

March 1

A successful missile attack against a TV station in Kyiv.[9]

Taking advantage of the fact that the regular work of television was disrupted, the aggressor resorted to intensifying information attacks.[10] In particular, the Security Service of Ukraine denied the message spread in social networks that the Russian military is installing mobile communication hardware that can allegedly interrupt Ukrainian networks. And the Center for Countering Disinformation at the National Security and Defense Council warned that the occupiers launched an information attack on the residents of Ukraine, mainly on the elderly, using phone calls to spread panic.

PRESUMPTIONS

1. Cyber and conventional attacks can be carried out simultaneously on the same object.
2. Cyber and conventional attacks can be aimed at gaining an advantage in the information space (i.e., depriving the civilian population of access to truthful information).
3. When conventional attacks on the means of access to information are successful (for example, when TV towers are damaged and TV companies are subjected to cyber attacks), the aggressor can increase the destructive effect by spreading disinformation and panic (by phone, on the Internet, etc.).

March 2

The Embassy of Ukraine in London suffered a cyber attack due to Russia's invasion of Ukraine[11].

The beginning of March

The beginning of March is the peak of Ukrainian activity in the international arena; the Embassy in the UK takes care of many issues (from implementing sanctions to supplying humanitarian aid).

On March 1, a powerful package of sanctions imposed by Britain against Russia following the full-scale invasion came into force[12].

Oliver Pinson-Roxburgh, CEO of Bulletproof and Defense.com, said: "The cyber attack on the embassy in London demonstrates that events in Ukraine are not taking place in a vacuum. Businesses worldwide must be prepared to deal with rapidly evolving threats, especially given the new malware targeting Ukrainian networks and hackers." The United States has warned its banks to prepare for cyberattacks amid harsh sanctions against Russia. Before that, Britain and the EU issued similar warnings to their financial institutions.[13]

PRESUMPTIONS

1. Cyberattacks have no geographical boundaries and thus scale the war in Ukraine to a conflict without borders.

2. Attacks in cyberspace can be directed against Ukraine's successful actions on the diplomatic front (as well as coincide in time with the decisions of Ukraine's international partners to strengthen sanctions).

March 16

The Red Cross of Ukraine reported hacking of its website, which was restored the same day. Thankfully, no personal data of beneficiaries were stored on the website. Only the information component of the site was affected.[14]

Due to numerous war crimes and the occupation of a large territory of Ukraine, the humanitarian situation is rapidly deteriorating. As a result, the role of the Red Cross of Ukraine is growing. In addition, the day before, on March 14, the leadership of the Ukrainian Red Cross (URC) met with the Delegation of the International Committee of the Red Cross in Ukraine (ICRC).[15] The URCS acted as a mediator between the ICRC and the Ukrainian government (which was especially important against the background of the ICRC's criticism, which only intensified in March).

Information attacks accompanied the cyberattack against the Red Cross.[16] In particular, social media began to disseminate information allegedly referring to the data of the International Committee of the Red Cross and reports of the Ministry of Defense of Ukraine that Ukraine "suffers enormous losses in manpower." Also, fakes began to spread about the Red Cross of Ukraine issuing certificates that allowed illegal border crossing.

PRESUMPTIONS

1. Russian attacks also target international humanitarian organizations.
2. The genocidal nature of conventional warfare leads to attempts of cyberattacks against organizations that could reduce the humanitarian crisis or the suffering of the civilian population.
3. Information attacks against international humanitarian organizations, which intensify cyber attacks, are aimed at destroying the image of such organizations, reducing the trust of the civilian population (which, accordingly, will lose the opportunity to receive humanitarian assistance due to distrust or unwillingness to apply to the relevant organizations).

March 28

Hackers carried out a powerful cyberattack on the infrastructure of one of the largest Ukrainian providers - Ukrtelecom. Ukrtelecom has seen a growing number of cyber attacks on its infrastructure since the beginning of the invasion of Ukraine.
The episode that took place on March 28 was powerful and complex. It took place `in two stages. The first was the discovery stage. The second stage was the cyberattack on March 28, during which hackers tried to disable the company's equipment and services and gain control over Ukrtelecom's network and equipment. The second stage of the cyberattack was detected within 15 minutes of the beginning. Ukrtelecom's IT specialists immediately took measures to counter the cyberattack. As a result, Internet access for customers was restored on the evening of March 28. The next day Ukrtelecom services became almost entirely available to all customers.

At the end of March, the conventional war was characterized by two trends.
On the one hand, the active phase of the war continued and intensified. But on the other hand, the Russian leadership had already become aware of significant failures at the front (primarily in the context of the collapse of the plan to capture Kyiv).

PRESUMPTIONS

1. Powerful cyber attacks can be used as compensators for conventional warfare failures.
2. Communication is the enemy's primary target, attacks against which can be carried out at any time.
3. Russia is capable of complex multi-step cyber attacks, but such attacks can be organized very rarely (due to the extensive resources required for preparation).

APRIL

April 8

Cyberattack on Ukrainian energy facilities.[17]

According to Ukrainian officials, the attack was planned to start on the evening of April 8 while residents were commuting back from work. The goal was to cut people from electricity and the internet, mainly the ability to check on the war news and the updates on their surroundings. Moreover, had the attack been successful, it would have cut power to an estimated two million people and made it difficult to restore power. [18]

April 8

The occupants launched a missile attack on the railway station of Kramatorsk.
The strike resulted in numerous casualties.

PRESUMPTIONS

1. An aggressor state can combine conventional and cyber attacks to increase panic attacks among the civilian population.

2. War crimes can be committed both conventionally and in cyberspace. Russian terrorism is also multi-dimensional.

April 11

cyberattacks on three European wind energy companies. The hackers tried to create chaos in a sector that is set to benefit Ukraine while reducing dependence on Russian oil and gas. The timing of the attacks suggests potential links to supporters of Russia's invasion of Ukraine.`

According to Deutsche Windtechnik AG, remote control systems for approximately 2,000 wind turbines in Germany were affected, with remote data monitoring connections to the wind turbines restored in 1-2 days. Operational customer service activities resumed on April 14 (3 days after the attack) and operated with only minor restrictions.

April 11

Statements by several countries about their readiness to refuse Russian oil and gas:

- Finland is ready to refuse gas and oil supply from Russia.

- France is ready to adopt a decision on a ban of Russian oil.

- Japanese energy company Kyushu Electric Power refuses to buy Russian coal. And Japanese insurance companies will not conclude contracts with companies operating in Russia.[19]

PRESUMPTIONS

1. The energy sector is vital for the Russian economy; moreover, it is the main element of Europe's dependence on Russia. Therefore, hacker attacks are aimed at green energy, which can shake Russia's position in the energy sector.

2. Hacker attacks may respond to states' political statements about their readiness to refuse Russian gas and oil.

3. Hacker attacks also aim to demonstrate green energy's "fragility" and instability.

April 14

CERT-UA reported the mass distribution of malicious XLS documents among Ukrainian citizens. Once they opened, they downloaded and launched "GzipLoader" and "IcedID" malware. "IcedID is also known as BankBot, a banking Trojan that can collect user credentials.

April 14

Foreign online stores and their acquiring banks block payments by Chinese UnionPay cards issued in Russia. [20]

PRESUMPTIONS

1. Russia can make simple but fast mirror cyber attacks.
2. "Mirror cyber attacks" can cover any sphere, including banking.

MAY

1 травня

Cyberattacks on online sales services and the support line of Ukrzaliznytsia.[21]

During the week, Russian and pro-Russian groups also attacked České dráhy (Czech Railways), some regional airports and the Czech civil service server, Estonia, Moldova, and Romania state resources, as well as Coca-Cola.

1 травня

On May 1, it was reported that the occupiers moved the weapons and military equipment, withdrawn from storage in the Western, Central, and Eastern military districts and the Northern Fleet. The railways were used for this purpose.[22]

PRESUMPTIONS

1. 1) Cyberattacks can be carried out against objects simultaneously used by the aggressor state for its own needs.
2. During the intensification of conventional operations, cyberattacks on the railway intensify, as it serves both as an object for evacuation and transportation of humanitarian goods and as an essential transport artery that provides the army (including foreign supplies).
3. Russia's cyber aggression is not only against Ukraine; Russia attacks other democratic EU countries to put political pressure on governments and reduce assistance to Ukraine.

May 9

Cyberattack on leading telecommunications companies of Ukraine. [23]

May 9

Massive rocket attack on Odesa. During his visit to Odesa, the President of the European Council, Charles Michell, was forced to go to a bomb shelter due to the air siren and the high probability of a missile attack. [24]

PRESUMPTIONS

1. On dates important for Russian propaganda, attacks on communication systems are likely. Cyberattacks can be used to strengthen propaganda.
2. Both missile and cyber attacks are used as retaliation for Ukraine's successes and as a tool to divert attention from Russia's failures. For example, the traditional parade in Moscow was less pompous and did not involve aircraft. Putin's regime uses multi-level attacks against Ukraine to demonstrate its success and strength to Russian citizens.

May 13

Massive cyberattack on the network of Lviv City Hall.

During the Russian cyberattack on the city hall network, part of the city's working files were stolen and published on enemy telegram channels. [25]

May 13

The shelling of Lviv.

Four rockets hit a military facility in the Yavoriv district. Those were destroyed entirely. [26]

PRESUMPTIONS

1. Conventional and cyber attacks can completely coincide geographically.
2. Simultaneous cyberattacks and rocket attacks on the same city are used to increase panic and negative consequences for the civilian population.
3. Cyberattacks against local authorities that precede the shelling can be used to discredit Ukrainian institutions.

May 14-15

Italian law enforcement repelled cyberattacks by pro-Russian groups during the Eurovision Song Contest in Turin, where Ukrainian performers won. [27]

Ukrainian band Kalush Orchestra won the Eurovision Song Contest 2022 final with the song "Stefania." After the performance, the band appealed to the world from the stage, calling to save the defenders of Mariupol from Azovstal (at that time, the defense of Azovstal continued).

PRESUMPTIONS

1. Russia carries out cyberattacks to inflict image losses on critical European cultural projects (i.e., it is a manifestation of humanitarian aggression).

2. Cyberattacks can also be predictive, that is, to counter possible Ukrainian information campaigns. It was obvious that Ukraine had a great chance to win. Given that the rescue of Azovstal defenders was a priority for Ukrainian society, the actions supporting Ukrainian service members were predictable. Therefore, the aggressor state uses all means (including cyberattacks) to prevent attention to its war crimes.

JUNE

June 2

Cyberattack on Ukrainian state organizations using Cobalt Strike Beacon malware and exploits for vulnerabilities CVE-2021-40444 and CVE-2022-30190.

The Governmental Computer Emergency Response Team of Ukraine (CERT-UA) detected the file "changes in salary with accruals.docx," which was distributed among the state. organizations of Ukraine by e-mail (computer infection with Cobalt Strike Beacon malware).

June 2

On June 1 and 2, the activity of Ukrainian officials with visits, speeches, meetings, and comments are monitored (activity during the All-Ukrainian Forum on Children's Day).

PRESUMPTIONS

1. Simple tactics, but the aggressor uses massive cyberattacks against civil servants to reduce the media activity of Ukrainian state bodies.

2. The aggressor can calculate that on specific dates (international holidays, memorial days, etc.) Ukrainian officials will make many statements, advocacy campaigns, etc. Therefore, cyber-attacks are prepared for these dates.

June 10

Massive cyberattack on Ukrainian media organizations using the malicious program CrescentImp.

In particular, mass emails were sent among Ukraine's media organizations (radio stations, newspapers, news agencies, and others) with the subject "LIST of links to interactive maps." As a result, more than 500 email addresses of recipients were identified.

A number of important international events are taking place around this time:

- Meeting of the EU-Ukraine Parliamentary Association Committee.
- The EU-Ukraine Parliamentary Association Committee is holding a two-day meeting in Strasbourg.[28]
- The European Parliament calls on the European institutions to grant Ukraine candidate status for EU membership.[29]
- EU summit: European Union representatives welcome stricter sanctions against Russia.[30]

PRESUMPTIONS

1. "International front" is essential to Ukraine's success. That is why cyberattacks against the media can occur in periods when active international activities are planned.
2. International advocacy is impossible without media coverage. Therefore, cyberattacks against the media are used by the Russian Federation to reduce the impact of relevant international events.

June 20

Cyberattack of the UAC-0098 group on critical infrastructure facilities of Ukraine.

A malicious document, "Imposition of penalties.docx," was detected, the opening of which will lead to the download of an HTML file and the execution of JavaScript code (CVE-2022-30190), which will ensure the download and launch of the Cobalt Strike Beacon malware.

June 20-21

Massive air strikes on the country's civilian infrastructure:

- Air strikes on infrastructure facilities near Bohorodichne, Ustynivka, Hirske, and Lysychansk, near New York; Shcherbaky (Kurakhove direction); near Ochakiv and Kutsurub in Mykolaiv region. [31]
- A strike on the Kharkiv subway depot. [32]
- Destruction of civilian objects in the Donetsk region. [33]
- 54 civilian objects - residential buildings and infrastructure - were destroyed. [34]
- In the afternoon of June 21, the enemy attacked the Industrial district of Kharkiv. [35]

PRESUMPTIONS

1. Attacks on civilian infrastructure can simultaneously occur in several dimensions, including cyber and conventional.
2. The aggressor state uses cyber attacks to multiply the adverse effects of missile attacks and increase the suffering of the civilian population.

June 24

Cyberattack against Ukrainian telecommunications operators using the DarkCrystal RAT malware.

Emails were distributed from an email address in the gov.ua domain (probably compromised).

When the document was opened, and the macro was activated, a PowerShell command was executed, which ensured the download and launch of the. NET loader "MSCommondll.exe". This executable file, in turn, downloaded and launched the DarkCrystal RAT malware.

It is assumed that the attack was aimed at operators and providers of telecommunications in Ukraine.

There are multiple essential events:

- Significant advance of the enemy on most directions, shelling, and air strikes. [36]
- Ukraine received the status of a candidate for membership in the European Union.[37]
- Russia's emergence of fakes and manipulations regarding Ukraine's candidacy for EU membership.

PRESUMPTIONS

1. Attacks against telecommunications operators can be used to strengthen the success of the aggressor state on the front (because communication is vital).
2. Cyberattacks on telecommunications operators also coincide with information attacks and the targeted spread of fakes about important geopolitical events (thus increasing the influence of fakes).

June 23

Russian special services attacked the e-mail server of Mykolaiv Regional State Administration. As a result, access was gained to the mailbox of the press service of the regional state administration.

June 22

Russian army shelled the southern city of Ukraine - Mykolaiv. [38] Russians launched seven missiles at the city.

PRESUMPTIONS

1. Conventional and cyber-attacks may coincide regionally (geographically).
2. Simultaneity of different attacks increases the negative impact on the civilian population and increases panic.

JULY

July 1

Cyberattack on the IT infrastructure of DTEK Group. It is a cyber-attack on Ukraine's most significant private energy company (which was carried out with missile attacks on the Kryvyi Rih power plant in eastern Ukraine).

On the evening of June 28, Russian occupants attacked the Kryvyi Rih thermal power plant. Russian propagandists announced this attack the day before, as the Ministry of Defense of the aggressor state announced the alleged Ukrainian military at the thermal power station.[39]

PRESUMPTIONS

1. Russia was actually "testing" attacks on energy infrastructure in the summer, which became bigger in autumn. In the summer, the aggressor state tried to find justifications for its attacks without directly admitting that its target was civilian infrastructure. In autumn, attacks on the energy sector were publicly acknowledged.
2. The simultaneity of cyber attacks and missile strikes against energy infrastructure is designed to scale the negative consequences and increase the damage from the attack.

July 6 and 11

UAC-0056 cyber attack on Ukrainian state organizations using Cobalt Strike Beaco.

These attacks coincided with critical international events. On July 4-5, the Swiss city of Lugano hosted a large-scale International Conference on Ukraine's Rebuilding. [40] On July 11, the Chairperson of the Committee on Ukraine's Integration into the EU took part in the Conference of the Chairpersons of the Parliamentary Committees on European Affairs of the European Union Member States (COSAC).[41]

PRESUMPTIONS

1. Cyberattacks on state bodies often coincide with the peaks of activity of Ukrainian high-ranking officials in the international arena.

2. Cyberattacks are aimed at reducing the effectiveness of international advocacy.

July 21

The TAVR Media radio holding stated that a cyberattack was carried out on the network of radio stations. As a result, it spread a fake message about the alleged severe health condition of President Volodymyr Zelenskyy was broadcast. [42]

July 21

The GUR stated that Russians plan to hold so-called "referendums" or otherwise annex the occupied territories to Russia, particularly Kherson and Zaporizhzhya regions.[43]

PRESUMPTIONS

1. Cyber attacks on media aimed at spreading disinformation are a constant element of Russian aggression. It is also an example of combining cyber and information attacks.

2. Disinformation calling to stop fighting is part of the overall policy to annex Ukrainian territories successfully.

AUGUST

August 16

On 16 August, the most potent hacker attack on the official website of the Energoatom Company since the beginning of the full-scale invasion of Russia took place.

August 16

Energoatom published information on the risk of radiation hazard violation at Zaporizhzhya NPP (Nuclear Power Plant). Macron and Zelenskyy also had a telephone conversation regarding the IAEA's proposal to send a mission to Zaporizhzhya NPP.

PRESUMPTIONS

1. Cyberattacks can be directed against a specific facility, which is also subject to conventional attacks and about which critical international negotiations are happening.
2. Nuclear terrorism in the Russian Federation is multidimensional and includes conventional, information, and cyber attacks.

August 18

Estonia suffered the most significant cyberattacks since 2007.[45]

August 16

Estonian government ordered the removal of six monuments with Soviet military symbols in Narva and its closeby areas.

PRESUMPTIONS

1. Cyberattacks are used by Russia to weaken Ukraine's allies.
2. Russian aggression also has a cultural dimension. The goal of the Putin regime is to preserve and spread its own worldview paradigm ("Russian world"). Therefore, cyberattacks are a response to attempts by any state to question Russian myths.

August 21

Russian hackers call to attack the Ministry of Digital Transformation.[46]

August 21

After Dugina's murder, Russian propagandists call for strikes on decision-making centers in Kyiv.[47]

PRESUMPTIONS

1. State authorities are the most common targets for Russian hacker attacks. This proves that the goal of aggression is to weaken and destroy the Ukrainian government.
2. Not daring to carry out conventional attacks on the central authorities of Ukraine, Russia resorts to cyber attacks (which are often a kind of revenge).

SEPTEMBER

September 16

Monobank, one of the leading banks in Ukraine, suffered a powerful DDoS attack.[48]

September 13

Monobank decided to abandon the Russian language in the application and announced that support for the occupier's language would disappear from the service.[49]

PRESUMPTIONS

1. The main advantage of Ukraine over Russia is the unity of civil society and business for a common goal. Therefore, pro-Ukrainian patriotic business is a potential target for hackers.

2. Russian attacks on Ukrainian businesses prove that the war's economic dimension is essential.

September 25

The cyber attack on Kyivgaz.[50]

September 26

A series of explosions on the Nord Stream gas pipelines.[51]

PRESUMPTIONS

1. Events in the cyber and conventional dimensions can be synchronized, meaning they occur in the same sphere.
2. Russia can use cyber attacks to strengthen its propaganda and misinformation attacks.

September 30

The website of the British counterintelligence service known as MI5 came under cyberattack on Friday by a group calling itself Russian Anonymous.[52]

September 20

The United Kingdom announced its intention to increase the amount of military aid for 2023. The intention was stated in a press release of the British government.[53]

PRESUMPTIONS

1. Russia uses cyberattacks on Western states as revenge for supporting Ukraine.
2. Russia carries out cyberattacks even against the intelligence services of nuclear powers (i.e., cyberattacks are considered an effective tool in case conventional attacks are too risky).

OCTOBER

October 8-11

October 8 - cyberattack on regional sections of the Ukrainian railway.

October 11 - cyberattack against transport and logistics organizations in Ukraine is occurring. [54]

October 11 - Russian hackers attacked the websites of American airports.[55]

October 8-11

October 8 - successful Ukrainian attack on the "Crimean bridge." [56]

October 10 - large-scale rocket attacks on Ukraine, including Kyiv.[57]

PRESUMPTIONS

1. Simple cyber attacks do not require much time to prepare, so they are often used as a quick response to the successful actions of Ukraine.
2. Russia's cyberattacks can mirror Ukraine's actions: after a successful attack on Russian infrastructure.
3. Russia carries out cyberattacks not only against Ukraine but also against its allies. The Russian Federation fears conventional strikes against NATO countries and dares to carry out cyberattacks even against the United States.
4. Cyberattacks and powerful missile attacks coincide in time, increasing the negative impact on Ukraine.

October 21

Distribution of e-mails allegedly on behalf of the press service of the General Staff of the Armed Forces of Ukraine. It is being distributed with a third-party link in it.[58]

October 20

Amid the intensification of rocket attacks, Commander-in-Chief of the Armed Forces of Ukraine Valeriy Zaluzhnyi stressed that the Ukrainian air defense and missile defense system is working thanks to the professionalism of Ukrainian soldiers and military assistance from partners effectively. He urged citizens to remain calm.[59]

PRESUMPTIONS

1. The primary purpose of attacks against civilians is to increase panic. That is why any attempts of the General Staff to counteract the enemy's information attacks are met with a response. In this case, there was an attempt to reduce the level of trust in the statements and messages of the General Staff.

2. The Commander-in-Chief of the Armed Forces of Ukraine enjoys tremendous support and confidence from the citizens of Ukraine. That is why attacks against him are predictable. Unconventional attacks, in this case, are aimed at weakening the military potential of Ukraine.

October 27

Marshal of the Senate of Poland Tomasz Grodzki reported a powerful cyberattack on the servers of the upper house of the Polish parliament.[60]

October 26

The Senate of Poland unanimously, by 85 votes, adopted a resolution on recognizing the Russian Federation government as a terrorist regime.

PRESUMPTIONS

1. Russia uses cyberattacks as revenge against Ukraine's allies for their support.
2. Russia is not limited to political (or diplomatic) responses to the political decisions of Western states; Russia's responses are disproportionate and hostile.
3. Cyberattacks against foreign governments demonstrate that Russia does not recognize any limitations or rules of its attacks.

NOVEMBER

November 24

Russia accompanies its missile strikes on Ukraine's energy facilities with powerful cyberattacks to cause a maximum blackout. According to SBU data published in November, on average, Russia carried out more than 10 cyberattacks on Ukraine per day (against critical infrastructure). [61]

In November, large-scale rocket attacks on energy infrastructure continued.

PRESUMPTIONS

1. Cyberattacks on critical infrastructure are aimed at amplifying the harmful effects of missile attacks.
2. The aggressor state considers the cumulative effect of various attacks on energy infrastructure as a tool to increase the suffering of the civilian population and panic.
3. Elements of genocide policy are not only conventional attacks but also cyber-attacks. Therefore, cyber attacks can also be war crimes.

November 23

President of the European Parliament Roberta Metsola said that the EP website was subjected to a cyberattack by pro-Kremlin hackers. [62]

November 23

The European Parliament recognized Russia as a state sponsor of terrorism.[63]

PRESUMPTIONS

1. Russian cyber attacks have no geographical boundaries. The Russian Federation does not risk conventional attacks on the EU but carries out cyber attacks.

2. Cyberattacks can be a response to any political decisions in the international arena that harm the interests of the Russian Federation.

November 24

the official website of the Ukrainian Greek Catholic Church, ugcc.ua was subjected to a DDoS attack by enemy hackers. In a few hours, 5 million requests were made, 1 million - every hour. Thanks to the timely measures taken by the IT specialists of the Information Department of the UGCC, the cyberattack was repelled. The work of the site has been restored.

November 22-23

the Security Service of Ukraine completed counter-intelligence (security) measures on the territories of the Holy Dormition Kyiv-Pechersk Lavra in Kyiv, the Korets Holy Trinity Monastery, and the premises of the Sarny-Polish Diocese of the UOC in Rivne region. In cooperation with the National Police and the National Guard, more than 350 church buildings and 850 people were thoroughly checked.[65]

PRESUMPTIONS

1. Russian cyberattacks may respond to Ukrainian security forces' successful security operations; such attacks are not always planned but may serve as revenge.

2. Cyberattacks used in response to Ukraine's successes are mirror attacks, i.e., they target the same area as conventional attacks.

3. Cyberattacks against the church prove that Russia considers this institution a political instrument of hybrid aggression.

TYPOLOGY OF CORRELATIONS

MATCHING BY SUBJECT

Geographical correlation

Different attacks occur against the same object or the same territorial unit.

Sectoral correlation

Different attacks occur concerting a specific sector; for example, energy, infrastructure, etc.)

TEMPORAL COINCIDENCES

Preparatory Attacks

(cyber attacks precede conventional attacks)

Synchronous Attacks

(cyber attacks amplify the harmful effects conventional attacks)

Retaliatory Attack

- ***Attack in revenge for Ukraine's success***
- ***Attack in against other states*** (to stop international support of Ukraine)

CONCLUSIONS AND RECOMMENDATIONS

Russian armed aggression against Ukraine began in 2014 and was multidimensional from the beginning. In addition, Russia has constantly used hybrid attacks (economic warfare, propaganda campaigns, etc.) to achieve its own goals. Furthermore, unconventional Russian aggression continues against Ukraine; such attacks are carried out against all "unfriendly" countries. These attacks pose global threats. Therefore, the correlation between different dimensions of aggression needs to be studied in detail, and all world powers (except for a few allies of the Russian Federation) are interested in effective counteraction to these attacks.

RECOMMENDATION 1

Ukrainian experience should be systematized and used to counter Russia and other authoritarian regimes.

Russia's large-scale invasion has demonstrated many logical connections between different types of attacks. The Russian aggression against Ukraine has no analogs in the modern history of Europe. At the same time, this war indicates the approaches that could be used in future armed conflicts.

The confrontation between democracy and authoritarianism is only gaining momentum and will be decisive in shaping the global agenda in the upcoming decades. Therefore, Ukraine's experience is the key to the victory of democracy. The main weakness of authoritarian regimes is that they use each other's experiences and are always similar.
Their centralization and predictability are not a strength but Achilles' heel.

RECOMMENDATION 2

Defence doctrines should adapt to the requirements of the times. Logical connections between different dimensions of Russian aggression can be used for forecasting and modeling.

Some of the data used to model the wars until February 24, 2022, were wrong. And it is not only that many analysts underestimated Ukraine and overestimated Russia. The problem is also that many theoretical assumptions have never been tested in practice.

Defense doctrines must consider that there are other ways to inflict significant damage on adversaries. And the more digitalized the world becomes, the more deadly cyber attacks can be.

Therefore, all strategic documents should consider modern warfare's multidimensionality.

RECOMMENDATION 3

International legal approaches to the legal definition of aggression should change (aggression in the XXI century is not only conventional). Moreover, responsibility should extend to all manifestations of aggression, not just the classic ones.

The legal definition of aggression was formulated by the United Nations General Assembly Resolution 3314 back in 1974. Since then, the international community has not dared to question the relevance of this definition. Unfortunately, international law also almost completely ignores the concept of economic aggression. Although Resolution 3314 provides that aggression is "the use of any weapon by a State against the territory of another State," there is currently no clear answer to whether "any weapon" includes economic, information, and cyber weapons. Most lawyers will have doubts. And this ambiguity is used by the aggressor state (and will be used by other authoritarian regimes). Therefore, the definition of aggression should be updated.

RECOMMENDATION 4

Cyberattacks can be equated to war crimes. Therefore, international humanitarian law should establish a stricter framework for unconventional attacks.

Russia's attempts to destroy the Ukrainian energy system have demonstrated t
hat cyber-attacks often accompany conventional attacks against critical infrastructure.
In theory, cyber attacks can cause no less harm and suffering to civilians than missile attacks. Consequently, cyber attacks can be war crimes. Thus, international humanitarian law should become more predictive and offer adequate regulation of the relevant legal relations.

RECOMMENDATION 5

The multidimensionality of Russian aggression proves the need for sanctions against the most critical sectors of the economy. Sanctions should be strengthened, and international companies should leave Russian market. Today, complicity in aggression is not only the sale of drones but also the provision of access to technology.

The power of unconventional attacks further exacerbates the need for complete economic isolation of the aggressor state.

In addition, peculiar aggression (primarily Russian cyber attacks) has no geographical restrictions. It means that Western companies that continue to supply Russia with the latest technologies not only contribute to the continuation of aggression against Ukraine. In addition, they undermine the security of their own countries because no one knows against whom a Russian attack will be launched tomorrow.

THE ECONOMIC SECURITY COUNCIL OF UKRAINE EXPRESSES GRATITUDE TO

the TRUMAN company and Department of Strategic Communications of the Office of the Commander-in-Chief of the Armed Forces of Ukraine for its facilitation and help with collecting and analysing data necessary for preparing this report.

Author:

Ilona Khmelova

Senior Research Fellow, ESCU

Independent Consultation:

Olena Yurchenko

Senior Analyst, TRUMAN

Denys Hutyk

Project Manager, TRUMAN

MATERIALS AND LINKS

1. https://journals.sagepub.com/doi/10.1177/0967010611431079
2. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details
3. https://www.rbc.ua/ukr/news/ssha-rassleduyut-kiberataku-sputnikovyy-internet-1647052748.html
4. https://disinfo.detector.media/
5. https://www.rbc.ua/ukr/news/ssha-rassleduyut-kiberataku-sputnikovyy-internet-1647052748.html
6. https://ukranews.com/ua/news/855983-za-godynu-do-vtorgnennya-rosiya-zavdala-masshtabnoyi-kiberataky-na-systemu-suputnykovogo-zv-yazku-v
7. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details
8. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
9. https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BB%D1%96%D0%BA_%D1%80%D0%B0%D0%BA%D0%B5%D1%82%D0%BD%D0%B8%D1%85_%D1%83%D0%B4%D0%B0%D1%80%D1%96%D0%B2_%D0%BF%D1%96%D0%B4_%D1%87%D0%B0%D1%81_%D1%80%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE%D0%B3%D0%BE_%D0%B2%D1%82%D0%BE%D1%80%D0%B3%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F_2022#%D0%91%D0%B5%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%8C
10. https://disinfo.detector.media/day/01-03-2022
11. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details
12. https://researchbriefings.files.parliament.uk/documents/CBP-9481/CBP-9481.pdf
13. https://cybernews.com/news/ukrainian-embassy-in-london-suffers-from-constant-cyber-attacks/
14. https://twitter.com/RedCrossUkraine/status/1504123401941790720
15. https://www.facebook.com/RedCrossUkraine/posts/1578656718837464/

16. https://disinfo.detector.media/search?search_string=%D1%87%D0%B5%D1%80%D0%B2%D0%BE%D0%BD%D0%B8%D0%B9+%D1%85%D1%80%D0%B5%D1%81%D1%82&-search_tag=

17. https://cert.gov.ua/article/39518

18. https://www.nytimes.com/2022/04/12/us/politics/ukraine-russian-cyberattack.html?utm_source=pocket_mylist

19. https://www.epravda.com.ua/news/2022/04/10/685535/

    https://www.epravda.com.ua/news/2022/04/10/685515/

    https://www.epravda.com.ua/news/2022/04/10/685514/

20. https://www.epravda.com.ua/news/2022/04/13/685666/

21. https://t.me/UkrzalInfo/2251

22. https://uk.wikipedia.org/wiki/Хронологія_російського_вторгнення_в_Україну_(травень_2022)

23. https://ukranews.com/en/news/856131-russia-carried-out-large-scale-cyber-attack-on-ukrainian-telecom-operators-websites

24. https://www.pravda.com.ua/articles/2022/05/9/7344951/

25. https://city-adm.lviv.ua/news/government/291555-naslidky-kiberataky-na-lviv-vykradeno-chastynu-danykh

26. https://t.me/andriysadovyi/765

27. https://hromadske.ua/posts/prorosijski-hakeri-atakuvali-yevrobachennya-ta-namagalisya-zlamati-sistemu-golosuvannya

28. https://t.me/verkhovnaradaukrainy/25217

29. https://t.me/verkhovnaradaukrainy/25297

30. https://t.me/verkhovnaradaukrainy/25196

31. https://t.me/mvs_ukraine/14194

32. https://uk.wikipedia.org/wiki/%D0%A5%D1%80%D0%BE%D0%BD%D0%BE%D0%B-B%D0%BE%D0%B3%D1%96%D1%8F_%D1%80%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE%D0%B3%D0%BE_%D0%B2%D1%82-%D0%BE%D1%80%D0%B3%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%83_(%D1%87%D0%B5%D1%80%D0%B2%D0%B5%D0%BD%D1%8C_2022)#/media/%D0%A4%D0%B0%D0%B9%D0%B-B:Kharkiv_Metro_depot_after_rocket_strike_on_20_June_2022_(02).jpg

33. https://t.me/mvs_ukraine/14202

34. https://t.me/mvs_ukraine/14238

35. https://t.me/mvs_ukraine/14260

36. https://t.me/mvs_ukraine/14329

37. https://t.me/verkhovnaradaukrainy/26789

38. https://t.me/mykolaivskaODA/1552

39. https://24tv.ua/udar-po-krivorizkiy-tets-golova-rva-pro-naslidki-ataki_n2052766

40. https://t.me/verkhovnaradaukrainy/28009

41. https://t.me/verkhovnaradaukrainy/28702

42. https://www.pravda.com.ua/news/2022/07/21/7359395/

43. https://www.pravda.com.ua/news/2022/07/21/7359429/

44. https://suspilne.media/271277-vtorgnenna-rosii-v-ukrainu-den-174-tekstovij-onlajn/

45. https://www.eurointegration.com.ua/news/2022/08/18/7145161/

46. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

47. https://www.pravda.com.ua/news/2022/08/21/7364186/

48. https://life.fakty.com.ua/ua/tekhnolohii/monobank-zaznav-potuzhnoyi-ddos-ataky-gorohovskyj/

49. https://life.fakty.com.ua/ua/tekhnolohii/monobank-vidmovytsya-vid-rosijskoyi-movy-chas-perehodyty-na-derzhavnu/

50. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

51. https://uk.wikipedia.org/wiki/%D0%A1%D0%B0%D0%B1%D0%BE%D1%82%D0%B0%D0%B6_%D0%BD%D0%B0_%D0%B3%D0%B0%D0%B7%D0%BE%D0%BF%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D1%96_%D0%9F%D1%96%D0%B2%D0%BD%D1%96%D1%87%D0%BD%D0%B8%D0%B9_%D0%BF%D0%BE%D1%82%D1%96%D0%BA

52. https://www.eurointegration.com.ua/news/2022/09/30/7147847/

53. https://www.gov.uk/government/news/uk-will-match-record-ukraine-support-in-2023

54. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

55. https://www.ukrinform.ua/rubric-technology/3590532-rosijski-hakeri-atakuvali-saj-ti-amerikanskih-aeroportiv-cnn.html

56. https://www.bbc.com/ukrainian/features-63183830

57. https://suspilne.media/291732-rosijski-raketni-obstrili-ukraini-10-zovtna-so-vidomo/

58. https://cert.gov.ua/article/2394117

59. https://www.radiosvoboda.org/a/news-hzaluzhnyy-ppo/32092725.html

60. https://www.eurointegration.com.ua/news/2022/10/27/7149503/

61. https://armyinform.com.ua/2022/11/09/ponad-10-kiberatak-na-strategichni-obyekty/

62. https://www.ukrinform.ua/rubric-world/3620523-sajt-evroparlamentu-zaznav-kiberataki-pisla-viznanna-rosii-sponsorom-terorizmu.html

63. https://www.ukrinform.ua/rubric-world/3620523-sajt-evroparlamentu-zaznav-kiberataki-pisla-viznanna-rosii-sponsorom-terorizmu.html

64. https://ugcc.ua/data/na-ofitsiynyy-sayt-ugkts-zdiysnyly-kiberataku-1500/

65. https://ssu.gov.ua/novyny/sbu-znaishla-prorosiisku-literaturu-miliony-hotivky-u-riznii-valiuti-ta-sumnivnykh-hromadian-rf-pid-chas-bezpekovykh-zakhodiv-u-prymishchenniakh-upts-mp-video