PER CONCORDIAM ILLUSTRATION

Lessons from UKRAINE

Russia's multilayered cyber assaults know no bounds

By **Col. Viktor Lisakonov**, chief of the Information Assurance Directorate, Ukrainian General Staff

Innovation has driven military strategy since the dawn of humanity. The inventions of gunpowder, the rifle-barreled gun and the combustion engine had huge impacts not only on military strategy, but on all of history. The 20th century was no exception. The evolving internet continues to expand the capacities of information technologies. But, as with other great inventions, its capabilities have frequently been used for negative purposes. The first computer viruses were created just for fun, but served as a warning for some and a criminal road map for others — cyber espionage, cyber attacks and identity theft are common now. However, there is a new aspect to the cyber threat.

On December 23, 2015, unknown hackers disconnected about 30 electrical substations in Ukraine, cutting power for about 250,000 people in the middle of a freezing winter. Before that night, no one had ever used cyber attacks against civilian critical infrastructure without an obvious monetary benefit. We now face a new threat with tremendous military and geopolitical potential. Within a short span of time, a single exploitation of systems vulnerabilities has evolved into an effective toolkit of hybrid capabilities with which to pursue a given geopolitical agenda. This reflects the new operational environment of cyber warfare, as Russia has demonstrated, using it to gain military and overall superiority in current and prospective conflicts. Understanding the threats, especially in their initial phase, serves a crucial role in choosing a successful response.

The notorious Gerasimov Doctrine was set forth in 2013 by Russia's chief of general staff, Gen. Valery Gerasimov, in "The Value of Science Is in the Foresight," published in the weekly Russian newspaper *Military-Industrial Courier*. This doctrine, which Russia implemented in Ukraine with oversight by Vladislav Surkov, a personal adviser to Russian President Vladimir Putin, implies the creation of chaos, inconsistency and internal conflicts. While instability and chaos-induction are not new to the Russian model of conflict resolution, Gerasimov and Surkov adapted it for implementation in the ongoing hybrid aggression against Ukraine. The use of cyber means, synchronized with a powerful propaganda base, political pressure and broad-spectrum military application, has been effective in causing instability in Ukraine.

From the beginning of the annexation of Crimea through the follow-on Russo-Ukrainian conflict in the eastern part of Ukraine, cyber operations accompanied all phases of aggression, especially kinetic operations. "In Ukraine, Russia has experimented with how best to produce military and political benefits from cyber

Masked Russian soldiers, also known as "green men," move toward a military base in Perevalnoe, Ukraine, in March 2014 after invading Ukraine's Crimean Peninsula. GETTY IMAGES

Two Russian soldiers, captured in the conflict zone in eastern Ukraine, stand trial in Kyiv in September 2015 on terrorism charges. REUTERS

operations," Kenneth Geers explains in his book, *Cyber War in Perspective: Russian Aggression Against Ukraine*. In *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*, James J. Wirtz describes the role of the cyber domain in Russian strategy: The "Russian Federation seems to have devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives." Key points for exploitation are lack of international legislative maturity, the complexity of the cyber domain and inherent anonymity. This approach allows the conduct of any manner of cyber operations to affect a harmful impact while leaving few traces or concrete evidence of Russian presence.

Throughout four years of Russian aggression, Ukraine has been under the constant pressure of cyber attacks in almost all spheres of life. However, attacks on critical infrastructure have evolved to be among the most dangerous and efficient in terms of potential and social impact. Seventeen years ago, security expert Bruce Schneier described a paradigm shift in his book, *Secrets and Lies: Digital Security in a Networked World*, which features a massive military application of civil technologies and infrastructure in place of conventional military assets. Use of the same computer systems by civilians and militaries implies that the same attack used against civilian targets could also be used against military targets. Given what has taken place in Ukraine, it is evident that attacks on critical infrastructure are among the most dangerous threats today.

Bureaucratic challenges

Perhaps the trickiest challenge of attacks on critical infrastructure is the immaturity of international legislation regarding cyber security and collective defense. Due to the relative novelty of the cyber domain, there is no appropriate legislative basis or vetting mechanism for the punishment of cyber criminals. An adversarial action requires an appropriate and proportional response, but a working mechanism for executing such a response does not currently exist.

A Ukrainian Armed Forces' cyber analyst scrutinizes NotPetya images in 2017. COL. VIKTOR LISAKONOV

Passengers wait to check their luggage at Boryspil International Airport outside Kyiv in 2017. The NotPetya cyber attack caused significant disruptions to business and daily routines in Ukraine. REUTERS

NATO's Article 5 implies that aggression against one member shall be met with a response by all members, including the potential use of armed force. As of July 2016, the Alliance began to recognize cyberspace as a domain of operations equal to air, land and sea. This means that an attack on any of the allies in cyberspace is grounds for a response, possibly an armed one. However, in the case of cyber attacks, attribution can be very difficult and complicated. How do you prove a suspect was the attacker? What evidence should be required? What types of attacks could be grounds for an armed response from the entire organization? Does NATO have procedures for handling these situations? A response option likely exists, but any decision could be rejected by one or more members. There are more questions than answers. That is why — across roughly 10 years of cyber attacks on critical infrastructure systems during geopolitical confrontations (starting with a massive series of attacks on Estonian public and private sector institutions in 2007) — there has been no solid precedent for officially attributing an attack to an attacker or means by which to punish an attacker.

This lack of clarity contributes to the increasing number of cyber attacks, and some nations successfully use this ambiguity to reach their geopolitical or military goals. Even though we traditionally think of critical infrastructure as civilian assets, hackers will not differentiate between civilian and military objects. In other words, cyber attackers will likely continue to take aim at critical infrastructure targets, regardless of whether the target is labeled civilian or military.

In addition, global security systems are based on coordinated responses to aggression. That means involving an international security body that discusses the problem, and then votes on and executes procedures. All of this consumes a crucial resource: time. Due to the nature and purpose of critical infrastructure, such long response times could bear too high a cost, such as humanitarian or ecological catastrophes resulting in the loss of innocent lives and destroyed environments. Such potentially disastrous impacts require imminent changes to response procedures.

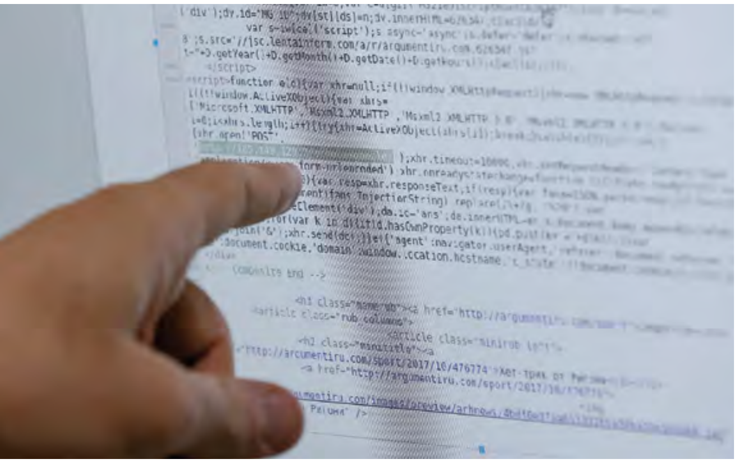
According to the Law of War as defined by the Geneva Conventions (and subsequently, by the Protocol Additional to the Geneva Conventions of August 12, 1949, and Protocol I of June 8, 1977), any attacks against objects of civilian infrastructure are strictly prohibited. These rules imply that attacks on civilian infrastructure include cyber attacks, although this has yet to be specifically spelled out within the Geneva Conventions. Potential anonymity in the cyber domain, along with legislative immaturity, provide free rein to groups and even state actors to operate in cyberspace with no punishment or regulatory consequences. The worst-case scenario would be civilian critical infrastructure being targeted to gain military superiority.

Growth of cyber attacks

After the "rebirth" of the Ukrainian Armed Forces, which included a significant increase in defensive capabilities and front-line stabilization, Russian cyber attacks became increasingly prominent in maintaining hybrid pressure on Ukraine. Not long ago, few could imagine causing the collapse of transportation infrastructure or cutting off a city's electricity in pursuit of geopolitical aims. Previously, only terrorist attacks were considered threatening to critical infrastructure, in the form of improvised explosive devices or similar conventional weapons. But now, the targeting of critical infrastructure via cyber means during a geopolitical confrontation is a reality. Ukrainian critical infrastructure assets have been attacked about a dozen times over a two-year period.

The most significant examples of such attacks include a citywide blackout in Kyiv, an attack on the western Ukrainian power grid, and attacks on Ukraine's treasury, Finance Ministry and railway administration and, of course, the NotPetya malware attack. It is important to note that all of these attacks mainly targeted civilians rather than military or government installations. The aim was to affect ordinary people in their daily routines by blocking ATMs, disrupting business processes and so forth. For instance, the treasury and railway administration hacks caused noticeable financial loss and transport delays. Practically none of the financial losses were incurred by the government, but there were problems for regular people who were not able to get tickets or money at Christmastime. These destabilization efforts were intended to degrade and handicap Ukraine from within.

The NotPetya attack was a massive campaign that affected the entire country through money losses, transport collapse, acts of intimidation and data leakage. The deep-dive analysis revealed its complex and multilayered nature, with a high cyber-component ratio. The extreme complexity, multilayered nature and coordination of the NotPetya campaign exposed the magnitude of state-level support for the malware attack. This campaign was not just an espionage campaign, nor just an operation to induce financial loss, nor a psychological operation. This was the practical use of cyber warfare as a major component of a hybrid operation, which in turn, is an implementation of the Gerasimov Doctrine. The takeaway from the NotPetya campaign is that cyber warfare dominance played an extremely important role in attaining superiority in this geopolitical confrontation.



A Ukrainian Cyber Police employee points to a malicious script used during a virus attack in 2017. REUTERS

In accordance with the Gerasimov Doctrine, Russia has intensively developed and widely used offensive cyber capabilities. A major part of these capabilities is directed toward critical infrastructure in order to affect ordinary people, making their lives more difficult and creating mass discontent. The main objective is to exploit a dominant cyber warfare position to gain advantage during geopolitical clashes. The approaches used in Ukraine could and probably will be used against Russia's other geopolitical opponents. In this respect, one of the main priorities is to protect critical infrastructure against cyber attacks. Adding to this is the challenge of preparing ordinary citizens for the near-certainty that they will be targeted in the event of a geopolitical confrontation.

Increasing severity, sophistication

The concept of using cyber attacks in a European country should be assessed in terms of whether such attacks are effective means for achieving geopolitical objectives. There has been an increase in the number, severity and sophistication of these attacks. For instance, during the Russo-Georgian War in August 2008 to disrupt communication between the Georgian government and citizens, Russian military cyber groups employed primarily low-technology distributed-denial-of-service (DDoS) attacks. Six years later, during Russia's occupation of the Crimean Peninsula, far more advanced types of attacks on telecommunication nodes in Ukraine caused traffic to be rerouted to Russian-controlled servers. Analysis of this information gave them an advantage in understanding and anticipating Ukraine's moves in the following military operations.

In addition, hackers quite effectively interrupted select connections between Ukrainian activists and international resources in order to isolate the country from international platforms. After the "hot phase" began, Russian tactics became much more sophisticated, and military critical infrastructure also increasingly came under cyber attack. These assaults started with several script-kiddie attacks (unskilled hackers using programs developed by others) on the backbone military network, and gradually advanced to well-crafted whale phishing (targeted against wealthy, powerful or prominent people) and social engineering attacks (psychological manipulation to get the target to inadvertently reveal secure information) against high-ranking officers. Also worth mentioning were the unrelenting cyber espionage campaigns that rapidly became more sophisticated and complex. The Operation Armageddon campaign, started in 2013, was a cyber espionage effort to harvest sensitive data. The aforementioned NotPetya campaign contained a wide spectrum of tools and techniques, including substitution of financial software updates with malicious ones, ransom demands and data wiping. Given the situation in Ukraine, it is hard to overestimate the consequences of data leaks to date. These attacks are usually not directed at specific institutions — military, state agencies or private sector. Therefore, mitigation of impacts is the most efficient response for coordinated efforts on the governmental level.

In the military sphere, Ukrainian cyber defense units have also noticed increased persistence and sophistication in attacks (target-tailored exploits, multivector attacks, customized complex malware, zero-day attacks, etc.) against military targets as well as critical infrastructure objects. Mitigation of such threats requires not only comprehensive and multilayered defenses, but also cooperation among "defenders," including civilian services

Forensic experts gather evidence after a car bomb killed Col. Maksym Shapoval, a top Ukrainian military intelligence officer, the same day the NotPetya campaign was launched. REUTERS

A Ukrainian boy gazes at a photo of his father, a soldier killed in the war with Russian-backed separatists, at a memorial service in Kyiv in 2017. THE ASSOCIATED PRESS

protecting critical infrastructure assets. To set up such cooperation venues at the state level, coordination and information-sharing systems should be reframed between government agencies and the private sector.

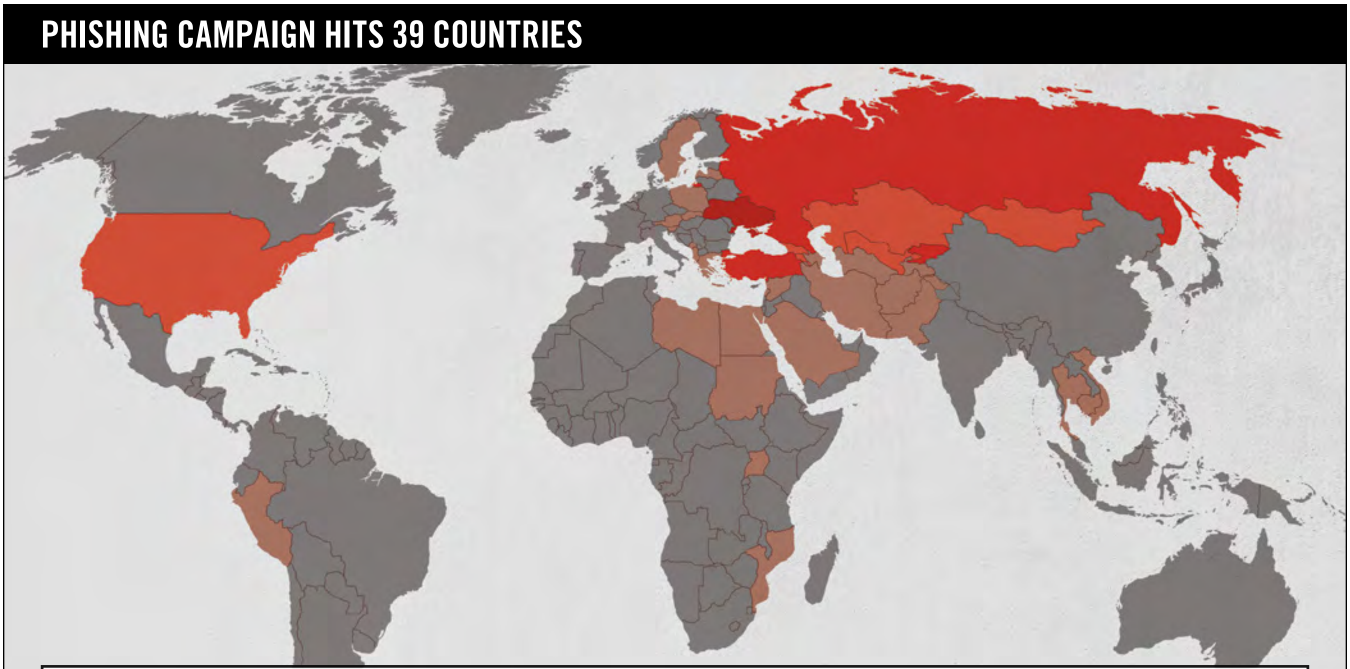
The past several years have seen an increase in the quantity and sophistication of cyber attacks against military and civilian critical infrastructure. This challenge is driving changes within the entire critical infrastructure cyber security system. For this purpose, coordination of cyber security by one state-level organization would be most efficient.

The changing threat

Analyses of cyber attacks against Ukrainian critical infrastructure reveal another interesting tendency. Increasingly, cyber attacks do not result in significant financial gains for the attackers. These attacks, most significantly, have a political resonance, social impact (increasing protest tendencies, manufacturing sympathy toward the aggressor), and degrade military capabilities (disruption of telecommunications, attempts to violate confidentiality in secure communications). This implies that the shift in attack vectors is achieving its desired results — namely, creating advantages that support a geopolitical narrative. Single hackers, usually involved in financial cyber operations, have not typically been able to orchestrate and conduct high-level cyber operations. For this reason, the conduct of cyber attacks against Ukraine's critical infrastructure is deemed to have evolved from individual hacktivists to organized, state-supported groups of highly experienced cyber experts, most likely with Russian support.

Over the past several years, advanced persistent threats (APTs) and state-supported groups of highly experienced cyber experts, capable of developing complex cyber weapons, began to appear. For instance, an FBI Joint Analysis Report on cyber attacks against the United States' 2016 elections identified two well-known Russian cyber-threat groups (APT 28 and APT 29) as the likely culprits. These groups have consistently focused on stealing intelligence for the Russian government. The majority of the cyber operations against Ukrainian critical infrastructure in the past few years were likewise most probably planned and

PHISHING CAMPAIGN HITS 39 COUNTRIES



TOP 10 COUNTRIES TARGETED

1	Ukraine	22%
2	Russia	11%
3	Turkey	7%
4	Kyrgyzstan	7%
5	Georgia	6%
6	U.S.	5%
7	Kazakhstan	4%
8	Mongolia	3%
9	Armenia	3%
10	Uzbekistan	3%

Source: The Citizen Lab

PER CONCORDIAM ILLUSTRATION

An extensive Russia-linked phishing campaign resulted in more than 200 stolen email accounts across 39 countries. Documents were used to manipulate data and plant disinformation.

conducted by these groups. They have repeatedly targeted Ukrainian, European and U.S. government marks such as militaries, international organizations, think tanks, media and others closely linked to Russian geopolitical interests and priorities. The main goal of such groups is to create and maintain a geopolitical situation favorable to Russia that, together with stolen data, is used by Russian authorities during military operations or political negotiations.

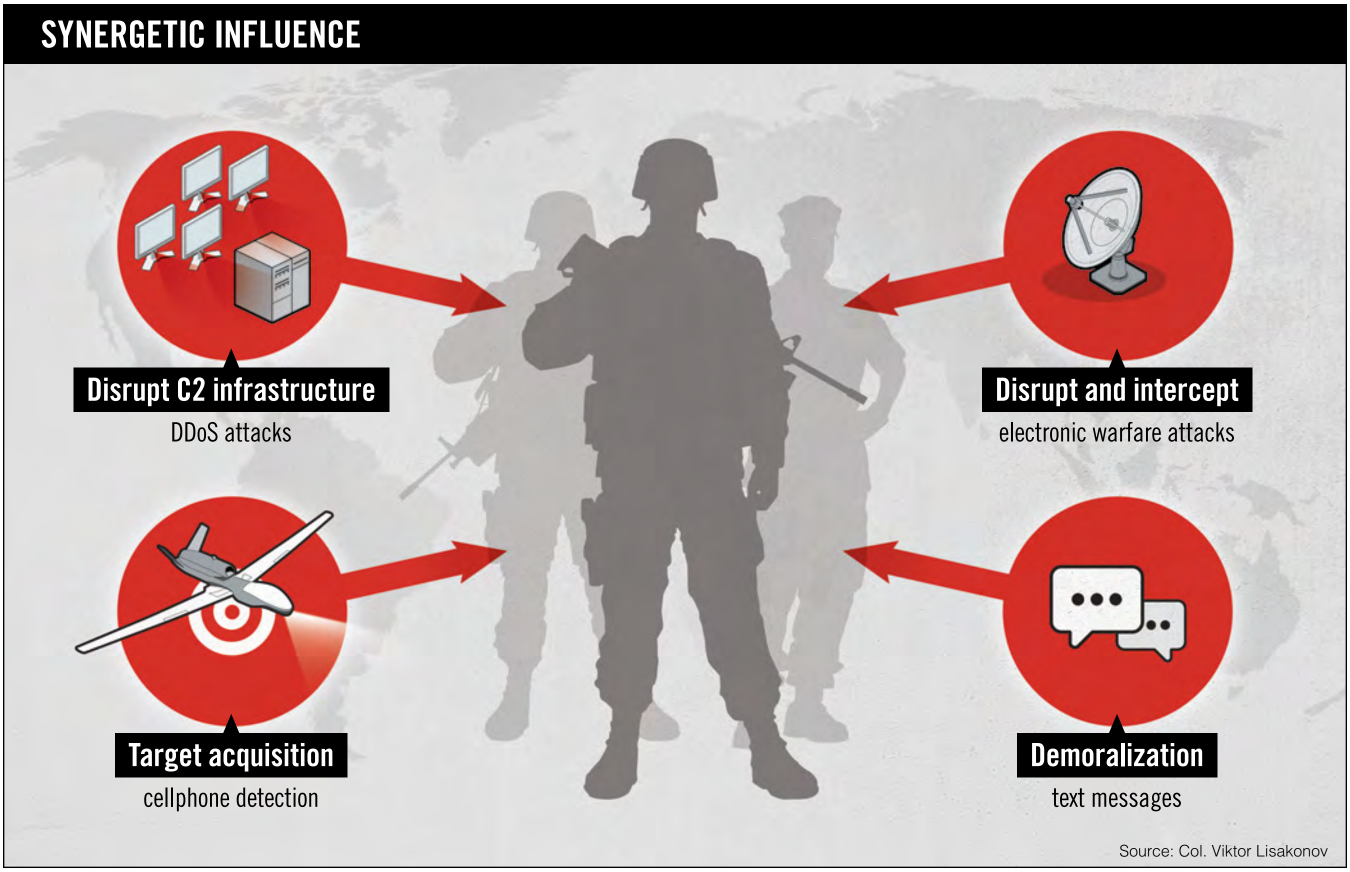
The threat shift from individual hackers targeting financial institutions to state-supported groups of highly organized and professional technicians targeting critical infrastructure occurred in recent years. This shift has had a major impact on the orientation, priorities and capabilities of cyber security systems everywhere. Only a couple years ago, financial institutions or wealthy corporations were the most lucrative targets for highly experienced hackers. Today, military facilities and critical infrastructure are among the most frequently attacked targets.

Synergetic cyber attacks

Another great challenge worth mentioning is the synergetic use of different types of conflict tools. The synergetic approach includes attacks coordinated in time, place and targets to amplify the effects of each other. This approach is not new and Russia has already successfully employed it in Georgia. In his article "Cyberwar Case Study: Georgia 2008," David M. Hollis describes this as "the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains." However, the cyber domain and its borderless nature and anonymity bring another variable to the equation in light of Russian aggression against Ukraine. The annexation of Crimea began with a series of disinformation campaigns intended to create ambiguity and despondency, and delay Ukraine's responses. Huge armies of trolls created the image of strong support from the Crimean population for Russian action, and the same picture was broadcast on Russia-funded international TV channels, such as Russia Today and Sputnik, for consumption by foreign audiences. At the same time, to ensure information superiority, Russian special forces physically destroyed cable connections with the Ukrainian mainland and took over the internet exchange point.

During the Donbas invasion, Ukraine faced a much more complex and sophisticated assault. Prior to the hot phase of the conflict, Russian intelligence and cyber espionage campaigns created a very effective background for future combat operations against the Ukrainian Armed Forces. Having acquired this advantage, cyber attacks, electronic warfare, and psychological and informational operations were well-coordinated with strong kinetic attacks. This synergetic use of various assets and methods across

SYNERGETIC INFLUENCE



Source: Col. Viktor Lisakonov

PER CONCORDIAM ILLUSTRATION

During major Russian operations, Ukrainian soldiers become the targets of complex, multidirectional influences that include electronic warfare and cyber psychological measures.

different domains enhanced the impact and frequently caused ambiguity among the attacked combat units. For instance, during Russia's Debaltseve offensive and the siege of the Donetsk airport, Russian specialists systematically broadcast demoralizing text messages to Ukrainian soldiers and their families. In addition, strong DDoS attacks were directed at command-and-control infrastructure, and tactical radio communications were interrupted by Russian electronic warfare. "During the 240-day siege of the Donetsk airport, the Russians were able to jam GPS, radios and radar signals. Their electronic intercept capabilities were so good that the Ukrainians' communications were crippled," Robert H. Scales wrote in his article, "Russia's Superior New Weapons." Traditional, powerful propaganda complemented the aforementioned. Social media were flooded with disinformation and panic messages. Hundreds of bots from troll factories and brainwashed pro-Russia individuals attacked the Ukrainian government and spread false stories about hundreds, or sometimes thousands of soldiers killed in action or captured.

This multilayered operation was coordinated in time, targets and objectives. A combination of cyber domain, electronic warfare, psychological and information operations, with simultaneous kinetic actions, damaged Ukrainian defense efforts. Taking into account the internal political situation in Ukraine and relations on the international stage, the synergetic use of such a wide spectrum of tools was a most effective strategy. But the most dangerous aspect of such an approach is that it is universal in scope and can be used to similar effect against any geopolitical opponent.

Conclusion

This author and his colleagues are directly involved in Ukrainian efforts to withstand such Russian hybrid aggression. The Gerasimov Doctrine entails the wide use of hybrid measures against an adversary to cause instability and internal conflict, just as it was executed against Ukraine. Objects of critical infrastructure are the most lucrative targets for such an approach. For the past decade, Russian offensive cyber capabilities have evolved from simple denial attacks to complex, multilayered operations that integrate simultaneous and coordinated usage of psychological, electronic and kinetic components, and financial and international pressure. A challenge in today's environment is that these offensive operations are neither fully understood by society and legislation, nor adequately addressed. This complex hybrid approach has potentially catastrophic impacts on critical infrastructure and the environment. Such attacks create disorganization, ambiguity and destabilization in society, which could create additional pressure on high-level decision-makers, leading to geopolitical benefits for the attacker. □