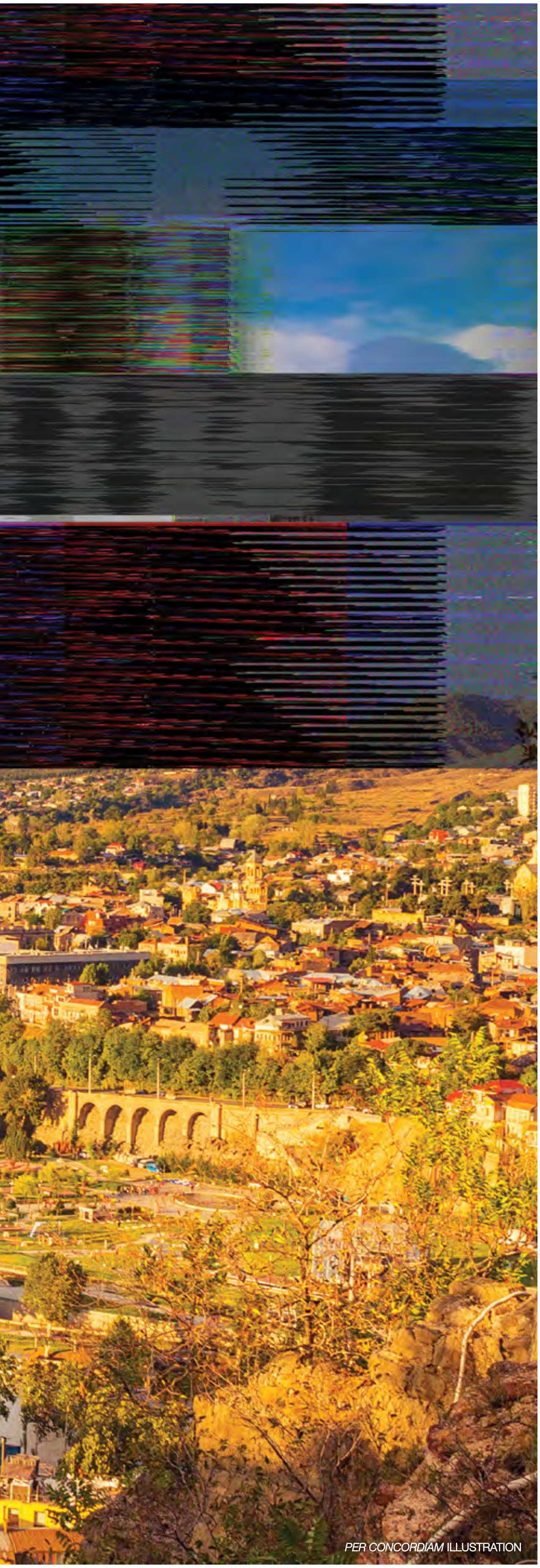
REBOOTING SECURITY



PER CONCORDIAM ILLUSTRATION

AN INNOVATIVE PLAN FOR PROTECTING GEORGIA'S CRITICAL INFRASTRUCTURE

By Andria Gotsiridze and Maka Petriashvili

In the 21st century, cyberspace has become the fifth domain of conflict, together with air, land, sea and space. Countries increasingly exploit cyberspace to achieve political or military goals or for geopolitical advantage. The number of states successfully developing offensive cyber capabilities is constantly increasing, and cyber warfare is rapidly becoming an integral component of war and conflict.

Russia, especially, has successfully integrated cyber elements into its hybrid war tactics. Its offensive cyber activities encompass all military, diplomatic, political, economic, social, cultural and religious areas, which it uses to exert technical and psychological impacts on its targets. As a result of experiences gained from conducting cyber attacks and information operations in Estonia (2007) and in Georgia (2008), Russia has evolved its offensive cyber tactics to its present-day application in Ukraine. Analysis of these conflicts proves that Russia uses conflict territories as training ranges on which to test its cyber-offensive capabilities.

A banner hangs in the main square in Tbilisi, Georgia, in August 2008, after Russian forces invaded the country. REUTERS

Cyber attacks against Estonia in 2007 were conducted to induce civil unrest. This was the first recognizable attempt to use a cyber attack to influence political processes. By the following year, during the Russo-Georgian war, Russia's cyber strategy had evolved into well-organized attacks, which were synchronized with conventional operations aimed at creating an information vacuum, spreading disinformation and blocking channels of international support for Georgia's government.

Russia's cyber-attack skill set has developed even further during the current conflict in Ukraine. Since the previous operations in Estonia and Georgia, Russia has acquired the use of large cellular operators for secret surveillance, which it uses to determine user location and other data. This data was broadly used for information gathering, psychological impact, and determining and transmitting locations for artillery strikes. For the first time, Russia attacked and shut down Ukrainian energy systems. Over the past two years, Russia has extended its cyber attacks beyond the post-Soviet countries, as hackers associated with various Russian government agencies have targeted election processes in the European Union and the United States.

SERIOUS THREATS

Russian cyber units pose a serious threat to Georgia. They are responsible for offensive cyber operations, including propaganda activities, inserting malware into an adversary's industrial control systems (ICS), and conducting specialized computer network operations and cyber activities on behalf of other units of the Russian armed forces.

Simultaneously, Russia is developing tools for remote access to critical infrastructure ICS. Anonymous actors have already managed to access and disrupt the ICS software of large companies by inserting malware.

After Russia's cyber attacks on Ukraine's energy systems, we can assume that a Russian offensive would not be limited to distributed-denial-of-service (DDoS) attacks, defacement and cyber espionage in future conflicts. There is no guarantee that attackers will not target critical infrastructure, which might lead to massive destruction and human casualties, even though low-level DDoS and defacement themselves may result in disproportionate losses to poorly protected infrastructure.

Together with network disruption and damage, Russia uses destructive cyber-psychological activities to influence an opponent's behavior and perceptions. Militaries prioritize the development of informational capabilities for war, peace or crisis situations to control information content and dissemination mechanisms.

The scale of the cyber threats that Georgia faces is increasing in terms of complexity and diversity, and Russian-orchestrated or -supported cyber attacks can lead to significant material losses and casualties. Cyber propaganda can negatively influence public opinion and perceptions among the Georgian people toward the West and, by forming and strengthening the image of the pro-Russian elite, foment a situation that might lead Russia to risk conventional military operations. Therefore, Georgia should pay special attention to creating and implementing information gathering and analysis mechanisms to better assess the intentions, capabilities and actions of Russia as a destructive cyber power/actor.

Locked Shields 2017, a cyber defense exercise organized by the NATO Cooperative Cyber Defence Centre of Excellence, took place inTallinn, Estonia. It is important for Georgia to participate in international cyber exercises. REUTERS

Ukrainian President Petro Poroshenko speaks in Tbilisi, Georgia, in 2017. Poroshenko, who has moved his country closer to the West, has been targeted several times by hackers. THE ASSOCIATED PRESS

CYBER RESERVE FORCES

It is vital for Georgia to integrate cyber capabilities and network protection into military operations. The country cannot afford not to staff its Armed Forces with qualified cyber specialists. A lack of cyber expertise is a common challenge within the public sector in general, especially for cyber defense. Information technology (IT) intellect is concentrated in the business sector, even in developed countries where public service offers greater pecuniary benefits than in Georgia, with its limited budget. Because cyber security is a common responsibility and critical infrastructure is primarily owned by the private sector, close cooperation between the private and public sectors is imperative, such as an effective public-private partnership model for countering crises during war and peacetime. Moreover, when the principal threat is a nation such as Russia, which broadly uses domestically grown hackers — with false personas such as CyberBercut, the Trolls from Olgino, and internetbots — public-private cooperation is indispensable.

In light of these threats from Russia, establishing a "cyber reserve" — a voluntary mobilization system for IT and cyber specialists employed in the private sector — is a purposeful solution. Such a cyber reserve could enable the state to mobilize nationwide cyber assets during war or crisis situations. Cyber reservists would employ their inherent knowledge and expertise in state emergencies. This system would also benefit the business sector, because IT specialists would have the opportunity to participate in various training and exercises typically available only to employees of state agencies. Such special skill sets are very important to effectively manage crisis situations such as those that resulted from the WannaCry and Petya viruses. As an example of best practices, Lithuania and Austria enlist IT specialists into their reserve forces, and Estonia very successfully deploys the essentially volunteer-based Defence League.

Cyber reservists would be recruited on a volunteer basis. The cyber reserve would consist of IT specialists from banks, internet providers, mobile operators, energy providers or other technology companies. These reservists would voluntarily serve and be called up via the Georgian National Guard. All recruits would be required to be certified in IT education and possess adequate skills and/or expertise to meet pre-established cyber reservist qualifications.

Their training would cover the general principles of information security and specialized cyber security issues. However, reservists would also be trained in basic combat and information operations skills. Cyber reserve service would be an alternative to compulsory military service.

Benefits to the state:

- Cyber defense capabilities enhanced to meet contemporary cyber challenges and threats.
- The Armed Forces acquires additional cyber and information operations capabilities.
- Cyber defense strengthened by integrating highly qualified IT professionals with minimal human resources and financial spending.

Benefits to cyber reservists:

- Opportunities to attend special state-funded training venues and exercises that are closed to the public.
- Opportunities to serve in the reserves as an alternative to compulsory standard military service.
- Maintaining and increasing professional proficiency while serving.
- Serving as a professional during war or crisis situations.

Benefits to the business sector:

- Employee qualifications improved via state-funded training.
- Company infrastructure better protected.
- Company employees exempted from compulsory military service.
- Cyber defense methodology development in business processes.

Projected outcomes:

- Development of additional Armed Forces cyber and information operations capabilities.
- Improvement of cooperation and coordination between public and private sectors.
- Integration of cyber elements into military operations.
- Integration of qualified personnel into national defense with minimal costs.

ОЩАДБАНК
вибачте за тимчасові незручності.
sorry for inconvenience.
извините за временные неудобства.
проводиться обслуговування
oschadbank.ua 0800 210 800
ГРОШІ
КАРТКА

A cash machine in Ukraine is knocked offline during a wave of cyber attacks against Ukrainian institutions in 2017. Ukraine has been heavily targeted by Russian cyber attacks. EPA

WOUNDED WARRIORS

In addition, the cyber reserve would represent an opportunity to reintegrate wounded warriors into the national defense. Georgia has about 1,500 wounded warriors from the 2008 Russo-Georgian War and from international peacekeeping missions in Afghanistan and Iraq who cannot serve on active duty due to their health. However, with training their inclusion in the cyber reserve would be possible.

Fundamental reasons for including wounded warriors in the cyber reserve:

- Georgia's wounded warriors have a high level of patriotism and desire to serve their country.
- Becoming a cyber defender allows them to reintegrate into society in meaningful ways.
- Their aptitude for tactics and strategy and understanding of physical battle tactics correlate to the cyber battlefield.

What will our wounded warriors gain?

- Remaining in the nation's service.
- Contributing to the enhancement of national cyber defense capabilities.
- Gaining cutting-edge skills in the newest and one of the most important security spheres.
- Continued active lifestyle.
- Compensation for services carried out for the country.

CONCLUSION

Cyberspace is a key element of hybrid tactics, and it is also used more and more widely in today's world, including in Georgia. Therefore, it is important to permanently include the cyber component in military exercises on the national level and to ensure that Georgia's state agencies and the private sector participate together in international cyber exercises. Effective cyber defense requires close cooperation between national agencies and private companies.

A cyber reserve project can and should be launched to provide strong support to this cooperation and to develop national cyber capabilities. Integration of private sector IT professionals into critical infrastructure protection will provide Georgia an adequate response capability to the destructive cyber actions of a powerful aggressor. □