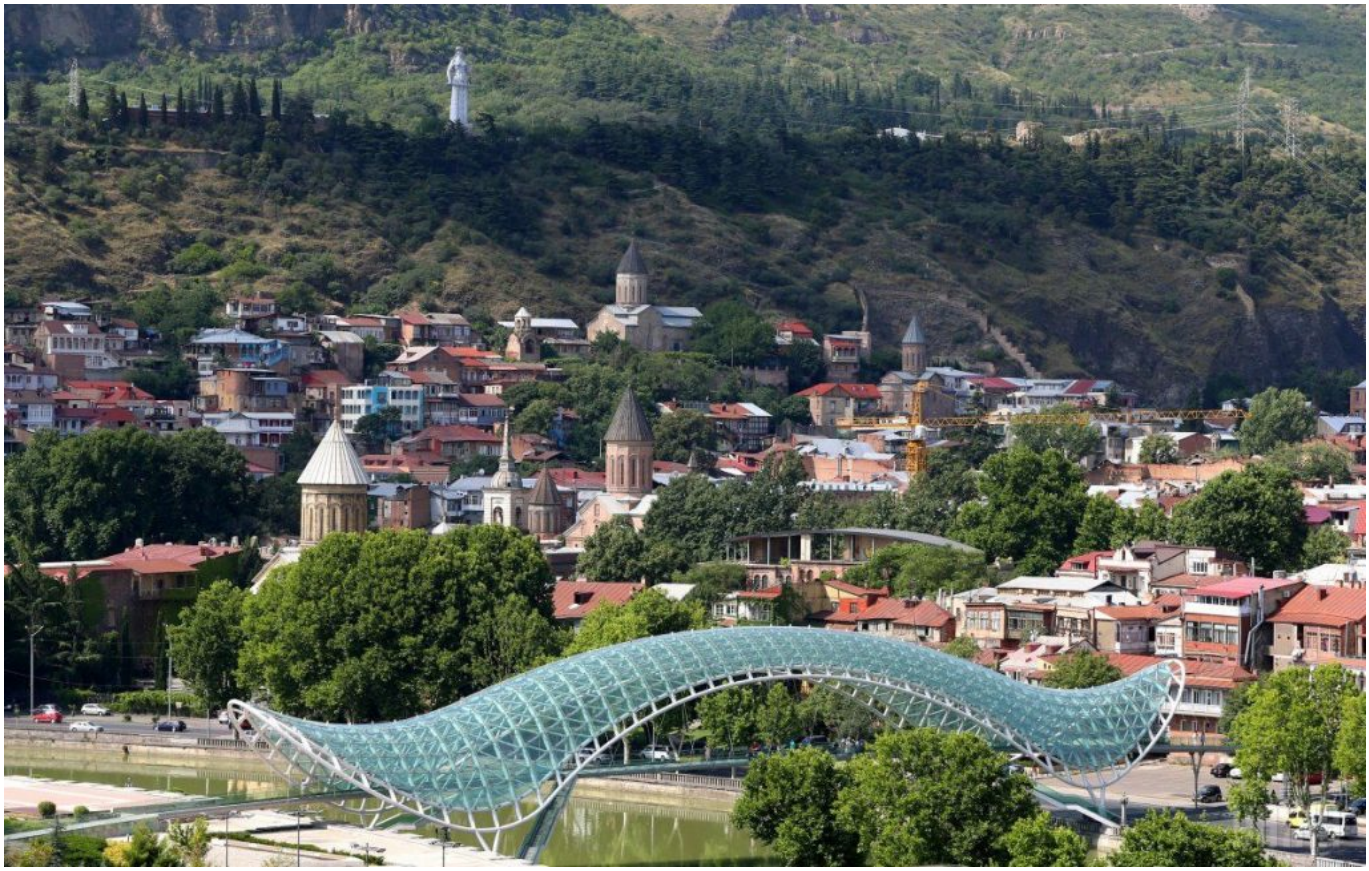
«Georgia and Kyrgyzstan are similar in myriad of ways, including Soviet past, lack of resources, turbulent political history, and other features when it comes to political and economic landscape of the two countries. Thus, it will be nothing but wise and useful for the government of Kyrgyzstan to examine the Georgian approach and experiences in the sphere of cyber security», – notes Nurbek Bekmurzaev, independent researcher, participant of the CABAR.asia School of Analytics from Bishkek.

The material was prepared as part of the internship program for participants of CABAR.asia School of Analytics in Tbilisi (Georgia).

Follow us on LinkedIn

---

1. Having adopted the concept of digital transformation "Sanarip Kyrgyzstan", the government of Kyrgyzstan finds itself in need to develop and implement comprehensive cybersecurity measures to ensure safe and successful digitalization;
2. Georgia has achieved significant success in a relatively short period of time in the sphere of ensuring cybersecurity and serves as a good example for Kyrgyzstan to model its cybersecurity program after;
3. As part of its cybersecurity strategy, the government of Georgia established an effective legal framework, built cybersecurity architecture from scratch, conducted awareness raising and training programs, and has facilitated local and international cooperation;
4. Kyrgyzstan can no longer afford to postpone adopting its cybersecurity strategy and other relevant legislation; the government needs to act now and do so with the consideration of the local context and international best practices and experiences;
5. Adopting strategies and laws is not sufficient though, the government should also establish research centers, develop training modules and awareness raising campaigns, and devise cooperation mechanisms with international partners and private sector at home.



In 2017, the ITU Global Cyber Security Index ranked it 2nd in the list of the most committed countries. In 2018, Georgia was ranked 9th in Europe and 18th globally in the Global Cyber Security Index. Photo: unian.net

In September of 2017, the Global Cyber Security Capacity Center published a report titled "Overview of the Kyrgyz Republic's Potential in the Sphere of Cyber Security". In short, the results of this study displayed a rather dire state of affairs by assigning low scores on all 5 criteria and stating that pretty much everything with regards to cyber security in Kyrgyzstan was still in the very early stage of development. Two years onwards and the situation has not changed much, but the need to change the approach to cyber security has become increasingly acute. This need is particularly apparent in the light of the government's decision to prioritize digital transformation projects. The recent adoption of the Concept of Digital Transformation "Sanarip Kyrgyzstan 2019-2023" and its Action Plan has set Kyrgyzstan on the path of digitalization, which promises to yield significant political, economic and social results.

While digitalization projects – if done right – do have numerous and considerable positive outcomes, especially with regards to making public administration more effective and efficient and boosting economic development, it also entails risks and creates multiple vulnerabilities in cyber space. Automating operations, creating information systems, and

connecting to internet exposes state agencies, businesses and individuals to cyber attacks. Thus, a crucial part of successful digital transformation will depend on ensuring cyber and information security, which will require establishing legal and institutional framework, raising awareness and educating all stakeholders, and cooperating with foreign and local partners alike. Unfortunately, the government's biggest achievement in this regard has been presenting a draft of a cyber security strategy in December of 2018; the document still has not been adopted.

However, an upside to being a late comer to cyber security is an opportunity to observe what other states have done so far, learn from their experiences and try to replicate their successes policies.

In this regard, Kyrgyzstan has a lot to learn from Georgia's approach and experiences in the sphere of cyber security. The government of Georgia is at the doorstep of adopting its third generation cyber security strategy. Georgia is consistently ranked among the top countries with well thought out and effective cyber security programs. In 2017, the ITU Global Cyber Security Index ranked it 2nd in the list of the most committed countries. In 2018, Georgia was ranked 9th in Europe and 18th globally in the Global Cyber Security Index. Georgia's success is even more impressive given how little it took for its government to join the list of leading cyber security countries – its first cyber security strategy was adopted 7 years ago in 2012. But it is not only Georgia's success that makes it a country for Kyrgyzstan to model its cyber security programme after. Georgia and Kyrgyzstan are similar in myriad of ways, including Soviet past, lack of resources, turbulent political history, and other features when it comes to political and economic landscape of the two countries. Thus, it will be nothing but wise and useful for the government of Kyrgyzstan to examine the Georgian approach and experiences in the sphere of cyber security.

What is cyber security? And why is it important?

Cyber security is the practice of protecting networks, systems, and data.

Specifically, it refers to availability, integrity and confidentiality of computer networks and information systems. In this case, availability of networks and systems refers to their operational status at all times when necessary. Integrity of systems and networks means that they remain unchanged and only authorized people can make changes to them. If you ever failed to install an outside program to your work computer, just know that you failed because doing so would compromise the integrity of the computer network at you work place. Confidentiality of system, networks and data refer to the rule that only authorized people have access to them to prevent theft, deletion and other types of damage. Ensuring

availability, integrity and confidentiality of computer networks, information system and data is the primary goal of any cyber security programme.

Recent political and security developments have led to the emergence of new types of threat in the cyber space. Cyber war, cyber espionage, cyber terrorism and cyber crimes are new additional set of threats states nowadays had to address. Hacking, malware intrusion, phishing and other forms of cyber attacks have made their way into everyday lives of companies and individuals. For states like Estonia and Georgia, which came under serious cyber attacks in 2007 and 2008 respectively, cyber attacks have been quickly elevated to the level of national security threats. However, even for countries Kyrgyzstan, which have not come under such large scale cyber attacks and do not find themselves in a hostile setting as Georgia does with regards to the ongoing military conflict with Russia, there are number of legit reasons for taking cyber security seriously.

First, only 12 percent of cyber attacks are state sponsored, meaning cyber war and cyber espionage comprise only a fraction of cyber crimes. Second, 80 percent of cyber attacks are directed at individuals, since humans have always been the weakest link in cyber security. Most cyber criminals pursue financial interests and steal personal data either for further theft from bank accounts, some sort of ransom, or selling it to other people. The fact is that digital solutions inevitable lead to cyber space and create vulnerabilities, which are guaranteed to be exploited by cyber criminals. Last, but not least, the current situation in eastern Ukraine demonstrates how friends can turn into foes in a short period of time and serves as additional impetus for designing and implementing proper cyber security measures.

Legal and institutional framework

One of the fundamental prerequisites to effective cyber security measures is legal framework. The nature of threats posed by cyber attacks and the relative novelty of those threats mean that the existing legislation does not cover cyber crimes or have mechanism for prevention and dealing with them. One way to classify cyber crimes is to look at them through a dichotomy of cyber-dependent and cyber-enabled crimes. Cyber-dependent attacks, such as hacking, malware intrusion or DDoS attacks, are offenses that can only be committed by using a computer, computer networks, or other forms of ICT. Cyber-enabled crimes are traditional offenses that are multiplied in scale or reach through the use of computer and computer networks. Georgia has developed legal framework from scratch to address cyber crimes, cyber war, and cyber espionage. It started by adopting the first cyber security strategy. The second generation strategy was adopted in 2017. Both strategies were aimed at establishing legal framework and cyber security architecture.

Simultaneously, the government of Georgia adopted two important laws: the first one on the Personal Data Protection and the second one on Information security – both were adopted in 2012. These documents allowed the establishment of new institutions, development of organizations, requirements and standards for ensuring cyber security of personal data, critical infrastructure and critical information systems subjects.

The above mentioned strategies and laws have led to the establishment of Georgia's cyber security architecture. The Council for State Security and Crisis Management of Georgia provides strategic direction and coordinates the work of relevant agencies in the sphere of cyber Security. The Law on Information Security led to the establishment of the Cyber Security Bureau (CSB) under the Ministry of Defense. This entity is responsible for ensuring cyber security of the country's military objects and organizations. Data Exchange Agency (DEA) under the Ministry of Justice deals with cyber security and information security in the public sector. It supports and monitors the implementation of the Law on Information Security by compiling a list of critical information systems' subjects and developing minimum requirements and standards for their protection from cyber attacks. As of now, the DEA has listed 40 state entities as critical information systems' subjects and applies comprehensive and strict cyber security measures to them. It is also responsible for running the Computer Emergency Response Team (CERT), which consists of IT specialists who provide technical support necessary for prevention and dealing with cyber attacks. The Cyber Crime Dimension (CCD) of the Central Criminal Police Department under the Ministry of Internal Affairs was established to investigate cyber crimes. In cases when cyber crimes are directed against the state, the CCD hands over investigation responsibilities to the State Security Council. Georgia's legal and institutional frameworks serve as strong foundation for implementing its cyber security policy.

Awareness raising, training and skills

For Georgia awareness raising and education has been one of the most important aspects when it comes to implementing policies in the cyber security field, considering the level of its novelty both for state officials and ordinary citizens. In short, most people are not aware of risks and consequences of visiting suspicious websites, clicking on questionable links and emails or downloading unknown files; it is not always easy to know when one comes under cyber attacks. Thus, humans have always been the weakest link in the cyber security chain. To prevent and timely deal with cyber attacks, the government of Georgia has launched mandatory training courses for all state officials. These courses are useful not only for educating purposes, but also for ensuring buy-in for cyber security programs from the top level government officials. Cyber hygiene courses for state officials teach them how to detect and avoid malware intrusion and phishing, to securely surf the web, as well as

educate them on cyber risks, types of cyber attacks and threats. There also table top cyber security exercises for the senior management, during which state officials work out different scenarios and courses of action in case of cyber attacks.

The DEA provides for the cyber security training needs of ordinary citizens and private companies. As part of its work, it organizes Cyber Security Forum twice a year. This platform provides opportunity to experts, state agencies and private companies to discuss challenges and exchange ideas. The fact that private companies own numerous critical information systems' subjects such as banks and internet providing services compels the state to organize cyber hygiene courses for private companies as well. University students are covered by the DEA courses too. Starting from 2020, it plans to introduce information security courses at schools and teach children about cyber security from early on. The Office of the Personal Data Protection Inspector organizes monthly free trainings and provides consultations on the data protection to companies and state agencies upon their request. All these state awareness raising and training programs, which are accompanied by complementary efforts from the civil society, stem from the underlying assumption that cyber security knowledge and skills are integral part of success.

International cooperation and public-private partnership

Whether it is cyber crimes, cyber war or cyber espionage, the novelty of cyber challenges has put states and private entities alike in a position where cooperation is not an option but an absolute necessity. Furthermore, the transnational nature of cyber attacks, coupled with its scope and frequency, serve as another factor why cooperation is a must. Georgia's main partners are European partners and the US. Georgia has been harmonizing its legislation with the European Union in an attempt to join it, and this involves co-operation in the cyber security field as well. Georgia has established close cooperation with Estonia, which hosts the NATO Excellence Center for Cyber Security, after falling victim to major cyber attacks in 2007. Another close partner is the US, which supports Georgia via enhancing technical capacities and raising awareness on cyber threats. The sheer variety and growing intensity of cyber attacks means that no state can effectively address them on its own.

An equally important form of cooperation is public-private partnership. Since the majority of cyber attacks are directed at individuals and private companies, it makes sense for the state to exchange information and solutions to these attacks. Most of Georgia's cyber intellect is in the private sector. In the context of dearth of well trained cyber security specialists working for the state agencies and concentration of many critical infrastructure objects and critical information systems' subject in private hands, it is of utmost importance to develop mechanisms and platforms for sharing information on cyber attacks, challenges and

exchanging best practices. There are confidential platforms for companies and state agencies to share information about cyber attacks without declaring damages – most companies are afraid of reputational damages. Moreover, to address the lack of cyber security, the government has attracted talent from the private sector to join its cyber reserve and be called in times of emergency due to cyber attacks. This cooperation mechanism solves the issue of preparedness to cyber attacks, lack of resources to pay them on regular basis, and the general shortage of cyber security specialist.

Conclusions

Georgia's approach and experience in ensuring cyber security teach three important lessons. First, it does not take very long to make significant progress, but it does take 'whole of the government' approach and constant political will. Second, it is important to establish legal framework and mechanisms for its amendment. Also, proper functioning cyber security programme requires cyber security architecture built from scratch – old institutions, organizations, and standards are neither adequate nor sufficient. Third, raising awareness and educating state officials, private companies and ordinary citizens ensures buy-in and success of cyber security measures. It is impossible to move ahead without people having knowledge and skills on cyber security.

With regards to recommendations for the government of Kyrgyzstan, these are 6 things it has to do first without further delay:

1. Adopt a cyber security strategy with clear goals and measurable objectives. The strategy should set feasible objectives and focus on laying the foundations in terms of legal and institutional framework.
2. Adopt a law on information security and other necessary laws and establish mechanisms for its revision and amendment. At this state it is important to keep in mind the importance of having a single coordinating state body.
3. Start establishing institutions and organizations that will become part of cyber security architecture. Do not assign cyber security responsibilities to the existing state agencies or do so only after extending their human and financial resources.
4. Establish research and analytical centers that will provide public, decision makers and stakeholders with knowledge and advice on how to move forward with regards to developing and implementing cyber security measures.
5. Develop awareness raising campaigns for the public and cyber hygiene training programs for representatives of state agencies and private companies that work in critical infrastructure objects and critical information systems' subjects.
6. Seek out friendly countries that have advanced cyber security programs and establish

cooperation to exchange experience and learn from their best practices. Simultaneously, establish mechanisms for public-private partnership.

This article was prepared as part of the Giving Voice, Driving Change – from the Borderland to the Steppes Project implemented with the financial support of the Foreign Ministry of Norway. The opinions expressed in the article do not reflect the position of the editorial or donor.