CYBER SECURITY THREATS AND RESPONSES

AT GLOBAL, NATION-STATE, INDUSTRY AND INDIVIDUAL LEVELS

Heli Tiirmaa-Klaar*

Although cyber security has accompanied the ICT sector since the first computer systems came into use, it was only in 2007, when large-scale cyber attacks came over entire nation, that the topic was catapulted to the centre of international attention. Estonia as a small, modern, technology-savvy country was an ideal test-ground for cyber attackers with political motivations. Estonia is often called the most wired country in the world, and it is true that the number of online services offered by private and public entities exceeds those in many other countries. For instance, 98% of the banking sector relies on electronic communications, over 90% people submit their tax declarations online, and government agencies use a unique e-government information system to do their daily business. Estonia's personal identification management system, which is based on electronic ID cards, facilitates many transactions between citizens and the state, as well as with private companies. Issuing an electronic signature is a routine task for most employees in the public and private sectors in Estonia.

Such high penetration of online services contributes to smoother administration and allows the country to cut down on many transaction costs in the economy. But as we witnessed in 2007, this system has also weaknesses that make the whole society vulnerable to computer network attacks. Estonia happened to experience the first large-scale attacks, but with increasing dependence on ICT-based solutions everywhere, the vulnerabilities are growing in both the developed and developing world. With the global telecommunications sector and world wide web, the interdependencies inherent in the system have bound us together, no matter where we are located geographically.

When someone asks for a single most important lesson from the Estonian cyber attacks, it would be undoubtedly be the need for more advanced international cooperation in cyber security. At the moment when 400 times more data are flooding your servers from all the countries in the world, the mitigation can be carried out only with the help of international contacts and networks. That's what has saved Estonia in 2007 from the worse. The Estonian Computer Emergency Response Team (CERT) contacted other CERTs, which, together with international informal information security networks, helped to neutralise the distributed denial of service attacks. At the same time, the Estonian information security specialists mitigated the attacks for three weeks on 24/7 basis to enable online services to run in Estonia. At the peak of the attacks, the Internet connection was limited with outside world for few days. It was a last resort measure that allowed to maintain online services inside Estonia. During these two days it was impossible to reach Estonia via Internet from outside world. At the time of heavy political campaign, with riots in the streets and propaganda attacks against Estonia over relocation of the World War II monument, disconnection from Internet added confusion as to what really happens in the country.

There are a few strategic implications that could be drawn from this experience. First, we have reached a point where the technology race has outpaced governments' ability to provide governance mechanisms over global telecommunication infrastructure and the Internet. As Estonia's case has showed, in 2007 the world lacked formal and institutional

cyber alert mechanisms and response systems for managing large-scale cyber incidents. The second important implication was that the issue of cyber security needs to be taken out from the IT departments' corner, brought to centre stage, and bolstered with political attention and extra investments in order to modernise protection mechanisms in most societies.

Estonia adopted a national cyber security strategy in 2008 that names promoting international awareness and establishing formal cooperation mechanisms in cyber security as central objectives, in addition to bolstering national cyber security efforts.

In order to conceptualise cyber security and develop protective policies, we need to divide the vast cyberspace into categories where the vulnerabilities are most likely to be present. One possibility for setting a mental framework for understanding cyber security would be to analyse cyberspace at various levels, each level indicating different consequences from cyber infrastructure disruptions. The consequences of cyber incidents and the appropriate response mechanisms are quite different at the global, regional and nation-state levels from those at the level of societal structures, economic sectors or individuals. But all these levels are tightly connected in cyberspace, and any effective response system needs to tackle all of them simultaneously.

Global or regional level

The most serious and far-reaching consequences will occur from information infrastructure disruptions at the global and regional level. Although the global and regional disruptions would hardly be the goal of any responsible international actor, they could theoretically happen as an unintended consequence of using cyber attacks as a part of conflict, possibly combined with physical forms of attacks For instance, if two regional rivalling powers are seeking to weaken each other, one of them (country A) could launch a large volume packet flooding attack, and a surgical cyber attack together with a physical attack towards the information infrastructures (e.g. fiber-optic cables, routers etc.) with an aim to disrupt the

economic activities in another country (country B) for political motivations. But since regional financial system could depend on the financial services provided by the country B, this would cause a serious disruption of services for nearby financial centres as well, causing a serious drop in the GDP of other countries in the region. As an unintended consequence, the rerouting of the data traffic via satellites and other connections would overburden the ICT sector capacities, which could lead then to different domino effects in other regions.

A very likely cause of a global ICT sector disruption would be also a technological failure. The preventive systems and countermeasures needed for recovering from the global technological failures are quite similar to those used when recovering from man-made catastrophies. Therefore, the international dimension and practical preventive mechanisms in cyber security cannot be underestimated.

At the global and regional level, the international incident response mechanisms and formal cooperation networks need to be formed by governments, international organisations and the stakeholder community of ICT sector companies in order to guarantee the incident management capabilities in the case of any global disruption.

Nation states

The second category of vulnerabilities concerns the level of nation states. A majority of current cyber policies are contained by national boundaries, and no viable international approach has emerged yet for the governance of cyberspace. Nation states are in an increasingly difficult situation since using cyberspace for warfare inhibits the principle of total asymmetry, if critical private and public information systems are attacked by a small group of IT professionals with advanced cyber methods.

One of the most feared conflicts in cyber space would take the form of a devastating cyber attack against a country's critical infrastructure together with physical attacks, which may or may not take place during a military conflict. However, cyber attacks during a (proper) military conflict will be less of a problem for analysts, since in the case of fully-fledged war it

will be possible to apply a framework of international laws that cover armed conflicts, and regulate the humanitarian aspects of a conflict. The Law of Armed Conflict and International Humanitarian Law set requirements to avoid casualties among the civilian population, refrain from non-proportionate responses, to consider secondary and tertiary effects etc.

The difficulty in a conflict between nation states where cyber methods are applied arises when military methods are not used in kinetic terms, the damage is achieved by cyber methods only, and the result is very serious but attribution of the attacks is almost impossible. A long discussion has been going on how to solve the attribution issue in a cyber attack. Although the forensics will always show the original sources, and point to people of a certain nationality or using certain equipment, these sources might have disappeared in the time since the legal process started and the attack chain from country to country was being investigated. Also, nation states or state sponsored actors could use proxy attackers located in territories without proper law enforcement, places with weak government structures and non existent national cyber monitoring systems, which makes attribution as foggy as possible and leads an investigation nowhere. Lawless “cyber heavens” exist and this is a known fact for nation states as well as for organised crime groups and terrorists.

A very likely scenario in future modern conflicts that include cyber methods is the use of members of organised crime or half-legal entities for organising and covering up attacks. It is still possible to lose traces and hide behind the fact that national regulations in criminalising cyber crime are very uneven, law enforcement personnel are overburdened in this area and there is not enough attention given to the issue of international cyber crime. At the moment, a well-equipped individual can launch a cleverly planned attack against whomever without getting caught.

Nation states also have to face the possibility of a terrorist attack that uses cyber methods or uses the combined powers of physical and cyber attacks to achieve the goal of an operation. Although anti-terrorist coordination among nations has been strengthened after 9/11 and most of the nations in the world are cooperating in this field, the likelihood exists that terrorist

groups will get the necessary know-how and use cyber methods in their operations. It is noteworthy that so far terrorists have not carried out any visible attacks against internet infrastructure. The reason could be the fact that they need the internet as a recruitment tool and do not want to harm the major medium facilitating their communication.

Most nation states are preparing for a classical computer network operation against the military communications infrastructure. Since this threat is not new anymore, most nations have secured their military communications reasonably well, and the risk for asymmetric attacks here is less of a concern compared to vulnerable civilian infrastructure.

All in all, nation states have already realised that the role of a traditional military will be decreasing in modern conflicts, and the role of the civilian crises management mechanisms will become an increasingly important tool for conflict prevention. In the field of cyber security, where more than 80% of information infrastructure belongs to the private sector in democratic countries, new crises management frameworks and public-private partnerships should be developed as a response to a new threat landscape.

In conclusion, at the nation state level countries need to bolster national cyber capabilities and develop resilient information infrastructure run by an educated national workforce. Governments would also benefit from developing an international information exchange, early warning and assistance mechanisms for swift reaction in times of crisis, as well as establishing a consultation framework with other countries.

Societal level

The third category of vulnerabilities relates to the societal effects of malicious activities on the internet. It includes social engineering that decreases trust among people, and also cyber methods that are used for agitating, terrorising, propagating or desinforming societal actors or certain groups in society.

Rapidly developing information and communication technologies have raised mass communication and its mediums to a prominent place in modern society. In an era where

news media is moving to the Internet and social communication is shifting to electronic chat rooms, any technological malfunction will affect a large number of people. Identity theft through social networks ranks as a the most common cyber threat in the last few years, and many people are not still aware of how to avoid these kind of attacks on their identity.

There are also certain trends concerning how internet could be part of future conflicts. Internet will increasingly be used during the conflicts as the medium to influence international public opinion or opinion of a certain country, or group within a country. Creating the media background with false contents, restricting the access to objective information and trying to avert the media attention will be likely methods.

A second trend of using the Internet based communication in a conflict is to spread the message among certain groups in society that their cultural values, religion or ethnic identity is being attacked.

To improve cyber security at the societal level, states can provide widely available public awareness training and assistance in information security, as well as effective law enforcement which will be able to cope with destructive campaigns on the internet.

Economic actors

The forth category includes economic actors, industries and sectors that are attacked for criminal or political reasons. The majority of attacks at this level are carried out for economic gains and with criminal motives. However, the increasing sophistication of cybercrime and the ease of using criminal groups as cyber proxies in attacking critical civilian infrastructure for political gains presents a growing concern for all decision-makers. Also, some companies might find themselves in an extremely vulnerable position when attacked by state sponsored actors with considerable resources.

In some sectors where cyber crime has been active for a long time, smaller companies are already heavily burdened by losses occurring from data theft and from additional administrative measures that should be applied to protect their clients' personal information

or assets. With increasing revenues from global cyber crime and criminal actors getting more organised, economic losses will present a serious risk for governments in the long run.

Companies in the financial sector are already investing into anti-fraud systems, and are used to bearing the consequences of the successful crime attempts. Other companies are securing their systems for preserving sensitive business information and preventing the loss of corporate secrets. As criminal organisations become more powerful, damage to the private sector might become a security concern in and of itself, without any nation state attack involved.

In most politically motivated conflicts in which cyber attacks will be used in the future, economic actors get hit in one way or another. The Internet traffic for botnets will be a matter for ISPs, insider threats and infrastructure exploits of critical infrastructure will damage private sector services and packet flooding attacks will be conducted against private sector even if they are intended to harm the government.

These fears have been addressed by few reports so far, but as the companies are not eager to disclose their real losses and many incidents are not publicly known, we may actually be seeing just the tip of the iceberg[1].

In order to strengthen the security of economic actors, governments can direct more resources for the fight against cyber crime, and strengthen law enforcement capabilities. Governments can also launch programs for training and educating the IT workforce and guaranteeing that companies have an environment where it is safe to operate.

Individuals

The last but still very important category that will be influenced by increasing malicious activities in cyberspace is average computer users. In most cyber incident scenarios the individuals will get affected by cyber disruptions and will suffer from the loss of services that

[1] "Virtual Criminology Report" Mc Afee, 2009

support their everyday life. With any man-made or technological cyber catastrophy most of the consequences could be quite unexpected, having secondary and tertiary effects. Even the most sophisticated approach cannot determine exactly all interdependencies between critical information infrastructures that support normal functioning of society.

Careless individuals represent also a threat in cyberspace if their unprotected computers will be used as part of hijacked computer armies, the botnets. Botnets could be used for attacking nation states, critical infrastructures and other industries. Additional serious vulnerability at the individual level that deserves attention is the negligence of employees. Human negligence and inadequate level of e-skills have originated at least as much security breaches in organisations as have external attacks.

At the level of individual computer users the awareness campaigns and national cyber emergency help desk could be helpful in achieving more resilient information society. Better public awareness will also contribute to the prevention of identity thefts and will decrease the number of people targeted by malicious activities in Internet.

Cyber security is very similar to traffic security where certain security culture is needed in order to achieve the situation where most actors behave lawfully. Creating cyber security culture can be accomplished only by raising awareness of all computer users. In this respect, all individuals have a great role to play in creating a more secure information society in the long run.

All the levels described above are vulnerable to cyber disruptions and attacks, which are easy to organise, hard to attribute, and asymmetric. Realising that the majority of the infrastructure is owned by the private sector and the majority of actors in cyberspace are companies and individuals, governments need to create effective public-private partnerships for securing cyberspace. The most effective response by governments could be to provide support for critical civilian infrastructure and to build a national cyber system that is resilient

in times of crisis. The broad base of civilian cyber capabilities, preventive mechanisms and efficient crisis management constitute building blocks of a national response system. Also, governments need serious national capabilities for advancing their fight with cyber crime, which poses a threat to their national and economic security.

All national mechanisms of individual states will be not be sufficient in the case of large-scale cyber crises and in fighting with international organised cyber crime. Developing international and regional information exchange, early warning and consultations mechanisms in cyber security are the long term challenges that governments will face in the 21st century.

***Heli Tiirmaa-Klaar, Senior Advisor to the Undersecretary of Defense Planning, Ministry of Defense Estonia**