INSS Insight No. 798, February 17, 2016

The Cyber Attack on the Ukrainian Electrical Infrastructure: Another Warning

Gabi Siboni and Zvi Magen

For some time, security experts have warned that critical services – for example, electricity and water supplies – can be attacked through cyberspace. The assumption is that such action requires sophisticated capabilities in cyber intelligence, technology, and operations, and possession of such capabilities is usually attributed to countries that have invested heavily in their development. Until now, even if in possession of such capabilities, most countries have shown restraint in using cyber tools to materially disrupt essential services and critical infrastructure in enemy countries. Events in Ukraine, however, question whether this assumption of restraint is still valid. On December 23, 2015, malfunctions were reported in portions of the electrical network in western Ukraine, after the operations of 27 distribution stations and three power plants were disrupted, causing the electricity supply system to crash. Many homes were cut off from the network. This was not a routine power outage: the Ukrainian authorities believe that a cyber attack originating in Russia caused the malfunction, and the Security Service of Ukraine (SBU) has blamed Russia specifically for the power outages.

It is difficult to prove with certainty who was behind the attack, but presumably the relevant authorities in Ukraine, with the help of Western agencies, will ultimately uncover the attacker's identify. The Ministry of Energy in Kiev has appointed a committee to investigate the affair. Thus far assessments concerning the party responsible for the attack are based on forensic examinations carried out on the damaged computers, which indicates that components in them were previously used by Russian groups. Furthermore, not surprisingly the technological capabilities point to a Russian element.

The conclusions of several security companies confirm the suspicion linking the attack to Sandworm, which according to the security company iSight is a Russian group affiliated with the Russian government. iSight has monitored Sandworm for over a year, and discovered that the group has collected information from the computers of Ukrainian administration officials, and from agencies in the European Union and NATO. Other

security experts reported that the group was also focusing on attacking industrial control systems. According to the security company ESET, located in Bratislava, the attackers used backdoor software that makes it possible to conduct operations on the target computers through a remote control server. In the Ukrainian case, use was made of a BlackEnergy component – a Trojan horse used as early as 2014 – to spy on Ukrainian administration computers and plant a malware program called KillDisk on power station computers in western Ukraine.

Hypotheses regarding a possible motive also support the suspicion that Russia is the party responsible for the attack, perhaps as part of the Russian campaign against cutting off the Crimean Peninsula, annexed by Russia, from electricity supplied by Ukraine. In addition, there is a great deal of information about the presence of advanced cyber warfare capabilities possessed by Russia and affiliated organizations, with Russia taking the lead in developing a combat doctrine that encompasses both kinetic and cybernetic activity. In the case of Ukraine, cyberspace operations enable Russia to continue denying its involvement in its neighbor, while at the same time persisting in efforts to attack it.

Effective wielding of the cyber weapon against sensitive targets in another country, in this case Ukraine, is likely to have far reaching consequences, not only for the future course of the particular conflict, but also for conflicts between other countries, or between countries and non-state organizations able to procure both offensive and defensive cyber capabilities. To be sure, similar cases of cyber attacks were recorded in the past. One of the best known examples of attack against infrastructure facilities that caused actual physical damage was the attack on Iranian nuclear installations with the Stuxnet software – alleged by some to have been carried out by Israel and the United States. Attacks in the Baltic states designed to prevent service were attributed to Russia. Nevertheless, the cyber attack in western Ukraine clearly reflects the use of this weapon against critical civilian infrastructure on a larger scale. This event, a precedent tantamount to crossing the Rubicon, is liable to serve as a model for imitation by other countries and perhaps organizations as well, while eroding the barriers of restraint that previously existed. In other words, it appears that the Ukraine incident is a sign that an especially important threshold has been crossed. Espionage, the theft of commercial information, financial crime, and denial of services are tolerable; although bothersome, they do not materially and directly harm the substance of daily life. An attack against the electrical infrastructure, however, can damage critical infrastructure and jeopardize human life. It therefore constitutes a quantum leap in the will to cause damage, in this case by a state.

Like other countries threatened in cyberspace, Ukraine will have to consider how to improve its defensive capabilities against similar events in the future. Israel can provide

an example here. Over the past decade, Israel has been able to develop advanced defensive capabilities for its critical infrastructure. Its defensive envelope includes gathering and analyzing intelligence and distributing it to the relevant agencies, as well as monitoring by the Israel Security Agency. This has created an environment of ongoing improvement and enhancement in defensive capabilities. Still, the proliferation of cyber capabilities, which has accelerated in recent years, enables new-old players – terrorist organizations and criminal elements – to acquire capabilities previously considered the exclusive province of nations. Concern is therefore growing that these non-state actors, which lack restraint mechanisms and state-like considerations, will attempt to imitate the model demonstrated in the attack on the electricity infrastructure in Ukraine.

Disruption of the supply of electricity is no trivial matter. It is enough to recall the events in Israel in late 2015 resulting from natural causes, and not a cyber attack: harsh winter weather caused serious disruptions over widespread areas lasting for many days. Israel is especially vulnerable in this aspect, due to the concentrated topology of its electricity grid. It is therefore necessary to continue monitoring related developments in Israel's strategic environment and throughout the world to assess whether there is a growing trend of cyber attacks able – despite sophisticated defensive measures – to inflict serious damage, and to prepare accordingly.