ISN
ETH Zurich

26 October 2012

The Challenge of Protecting Critical Infrastructure against Cyber-Attacks

Cyber-attacks on critical infrastructure represent a threat to both governments and the private sector. Since small countries such as Switzerland are especially vulnerable, argue Daniel Stauffacher and Barbara Weekes, international mechanisms to deal with these cyber-threats are necessary.

By Daniel Stauffacher and Barbara Weekes for ISN

There has been a lot of discussion recently on the possible consequences of a sophisticated cyber-attack on critical infrastructure. In response, it has been suggested that this discussion – much of which is not based on real intelligence about legitimate or known threats – amounts to little more than hype and scaremongering that is, in turn, used to justify a heightened state of security. While there is some basis to such criticisms, they nevertheless miss the point. Governments that are accountable to their citizens must be prepared for “worst case” scenarios, or risk being accused of irresponsibility. In addition, the biggest danger in the realm of critical infrastructure protection is the absence of internationally accepted mechanisms for dealing with cyber-conflicts and attacks.

No one can deny that the functioning of governments, cities, corporations and ultimately of the global political and economic system relies upon unfettered access to the Internet and a complex network of information and communication technologies. Cyber-attacks have the potential to compromise such access because they are often difficult to detect, may go unnoticed for many years, and offer the perpetrator the possibility to attribute the attack to a third party. Moreover, cyber-attacks are often instantaneous and global; data packets can reach the entire world in less than half a second and are not subject to unified international legal standards. This means that cyber-attacks represent a new type of conflict, in which it has become far easier to attack than to defend.

Governments and corporations, in particular those operating privately owned critical infrastructure – for example, transport, communications networks, pipelines and financial institutions – have become a clear target for cyber-attacks. And as a key provider of electricity and an important banking and financial centre, Switzerland is undoubtedly at risk of attack. Whether via a USB stick or a direct internet connection, corporations and governments are vulnerable to external actors with the requisite know-how. The explosion in the use of personal devices and the ubiquity of technology and connectivity in all aspects of life have made systems increasingly vulnerable. These weaknesses are compounded in many critical infrastructure installations by outdated security measures & IT systems, a lack of preparedness or early warning systems, and institutional obstacles to sharing information.

High Stakes

The high stakes of cyber-attacks on critical infrastructure have become increasingly evident as a result of 1) Stuxnet (2010), which was used by the United States and Israel to attack computers controlling centrifuges at a uranium enrichment facility in Iran, 2) incidents related to Flame (2012), which was used to attack computers at strategic oil facilities in Iran, and, most recently, 3) what are thought to be Iranian cyber-attacks on US banks and an oil firm in Saudi Arabia. In October 2012, US Defense Secretary Leon Panetta likened the potential impact of cyber-attacks on critical infrastructure to that of the Pearl Harbor attack in 1941. He also revealed that the United States is developing rules that will allow the military to launch pre-emptive digital strikes if necessary. That path, however, is fraught with difficulty, as there is no recognized international procedure to manage these kinds of incidents, or any real mechanism for assessing collateral damage to corporations, organizations or individuals once cyber-weapons make their way ‘out’ of intended targets and into the broader online community.

Several multilateral initiatives for managing cyber-threats currently exist – most notably the United Nations Group of Governmental Experts. The Organization for Security and Cooperation in Europe (OSCE) is also currently promoting a list of possible confidence building measures (CBMs) that define ‘off-limits’ areas for cyber-attacks and share situational awareness and communications systems. Unfortunately, progress in these and other international fora is slow and does not reflect the urgent need for systems to prevent and mitigate the escalation of cyber-conflict. Unless greater progress is made, these discussions will always be playing ‘catch-up’ to the rapidly evolving realities on the ground – and that means that the nations with the most “cyber-power” can dictate the rules of the game.

Challenges and Responses

The most significant challenges associated with cyber-attacks on critical infrastructure are those of attribution and third-party involvement. First of all, the difficulties of attributing cyber-attacks need to be accepted in order to move the debate forward, and systems need to be established that take these challenges into account. This situation is complicated further by the involvement of third-party countries or individuals, who may be unaware that an attack has emanated from their territory or device(s). As recently reported by MELANI – the Swiss Government’s Reporting and Analysis Centre for Information Assurance - the Flame virus that was used to attack Iran actually went through Switzerland. This demonstrates that international norms and an accepted framework for how to manage these complex challenges are urgently needed. One possible system would be to entrust states with the responsibility to investigate suspect activities and attacks emanating from cyber-infrastructure located within their territory. Depending on the scale of the attack, the aggressor could then be punished under national cyber-crime legislation (where it exists) or other applicable legal codes.

There is also evidence that certain types of industrial control systems are particularly vulnerable to cyber-attack. According to Vartan Sarkissian, senior advisor at the East West Institute (EWI), a significant number of attacks have occurred against Supervisory Control and Data Acquisition (SCADA) systems. These are vulnerable because they frequently rely on outdated information technology that is easily hackable. In fact, some SCADA control boxes are still so basic that Distributed Denial of Service (DDoS) attacks can be easily achieved. To make matters worse, SCADA systems tend to be infrequently patched, despite awareness of the risks.

In addition, many critical infrastructure installations, such as electricity distribution systems in Switzerland and in many other countries, are divided into segments provided by different companies operating with different systems. In principle, this could be good for security as a variety of systems makes it harder to carry out attacks on a one-size-fits-all basis. In practice, however, security at most installations is minimal due to the high costs created by this fundamental architectural problem. At the highest power grid level in Switzerland, a unified system is currently being implemented by Swissgrid to ensure secure and reliable distribution both at home and internationally.

Finally, the importance of the user in every security situation cannot be neglected. Whether through accidental misuse, Internet activity, working from home, infected USB sticks, malicious approaches via social engineering, or ‘passwords on post-it notes’, the company employee remains the weakest link in the defence of any nation’s critical infrastructure. In addition to carelessness, there is also the risk of a disgruntled employee who physically or electronically leaks data outside the company or organisation. An example of this recently occurred at the highest level in Switzerland when an employee at the Swiss intelligence agency (Nachrichtendienst des Bundes (NDB)) uploaded large amounts of confidential information onto hard drives and removed it from the premises.

The Challenges Facing Small States

Because attacks on critical infrastructure are relatively easy to carry out, determining the appropriate response can be challenging, especially in the case of smaller countries like Switzerland. The cost of creating an optimal defensive system is extremely high for any organization, and becomes an even more significant hurdle in the context of restricted budgets, limited resources and a lack of trained personnel. Solutions therefore need to be pragmatic and geared toward defense, managing risk, protecting business continuity and, as a last resort, offensive action. At both the national and international levels, working groups that bring together law enforcement agencies, the military, government and the private sector can help to facilitate the establishment of early warning systems and the exchange of information and best practices.

Despite having to accept a certain degree of unavoidable risk, operators of critical infrastructure need to implement corporate plans and participate in sectoral, national and (where necessary) international arrangements to prevent and mitigate attacks, and to ensure continued delivery of services in case of emergency. Private sector organizations in particular must ensure regular updates of IT security measures, implement adequate encryption systems, define responsibilities down to the level of the individual user, and ensure that individual users can only go online when security measures are activated.

Daniel Stauffacher, is a former Delegate of the Swiss Federal Council and Swiss Ambassador to the United Nations. Currently, he is President of Dr Daniel Stauffacher + Partner, Consultants (www.stauffacherconsulting.ch). Dr Stauffacher is also a founder of the ICT4Peace project, and inter alia on the board of the World Wide Web Foundation.

Barbara Weekes is a Senior Advisor for the ICT4Peace Foundation, Switzerland. She is also Chief Executive Officer of the Geneva Security Forum and was an executive at the World Economic Forum from 1995 to 2000.

Publisher

International Relations and Security Network (ISN)