Stealth war on the Internet

Nations must act together to promote cyber peace

By Myriam Dunn Cavelty and Oliver Rolofs

DIE KLEINERT.DE/TOM STEYER

For more than a decade, different forms of cyber conflict have accompanied every political, economic and military confrontation. Criminal and espionage activities carried out with the help of computers happen every day. Given the constant high-level of coverage for such events, it is not surprising that cyber war has become a media and political buzzword: A rapidly growing number of countries considers cyber attacks by non-state or state actors to be one, if not the major (future) security threat.

PATRICIA SCHELLER

Myriam Dunn Cavelty is Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich, and Fellow at the stiftung neue verantwortung, Berlin.

PATRICIA SCHELLER

Oliver Rolofs is the Press spokesperson for the Munich Security Conference and Associate at the stiftung neue verantwortung, Berlin.

Cyber War or Cyber Diplomacy

Last year, the tenor of the debate changed discernibly. The main culprit is the worm also known as "Stuxnet," a sophisticated programme believed to have been written to sabotage systems that control and monitor industrial processes. Though the world may never know for certain who is behind this piece of code, Stuxnet has irrevocably shifted the cyber war paradigm. The majority of strategic planners out there are willing to believe that one or several state actors – Israel? The US? – were behind the computer virus and that they deliberately released it to sabotage the Iranian nuclear programme. For those people, cyber war is no longer pie in the sky – it is reality; a 'digital first strike' has occurred.

This belief has become so strong that it seems almost pointless to rally against it. The phantom of cyber war has great appeal because it seems modern; because it promises quick wars without suffering and immense budgetary advantages; because it enables governments to get rid of outdated and inefficient Cold War defense equipment while at the same time investing in human capital and knowledge to keep their countries safe.

In addition, the term is frequently used for almost any phenomenon involving a deliberate disruptive or destructive use of computers. And because there are so many of these occurrences every day, it does indeed look as if the developed world is facing an enormous problem.

But most of these events have very little to do with war, though they often accompany conflict-like situations. In fact, in the history of computer networks there are only very few examples of severe attacks that had the potential to, or did disrupt the activities of a nation state. There are even fewer examples of attacks that resulted in physical violence against persons or property.

Though dubbing these activities cyber war might be an often thoughtless and essentially harmless act by most, the use of the word "war" by state officials in the international arena bears an inherent danger: Implicitly or explicitly moving an issue into the realm of national security and military actions is to subject it to the rules of an antagonistic zero-sum game in which one party's gain is another party's loss. In addition, though deterrence language does not really work in the realm of cyberspace, many states have begun to toughen up rhetorically.

As a result, the first signs of a cyber security dilemma are becoming apparent: Athough most states still predominantly focus on cyber defense issues, measures taken by some nations are seen by others as covert signs of aggression. That leads to more insecurity for everyone – specifically because it is almost impossible to assess another state's true cyber capabilities. Therefore, even if we judge the possibility of a "real" cyber war to be negligible, the current situation is influenced by the old, familiar Cold War arms race dynamics, which are detached from the reality of cyber capabilities generally and cyber weapons specifically.

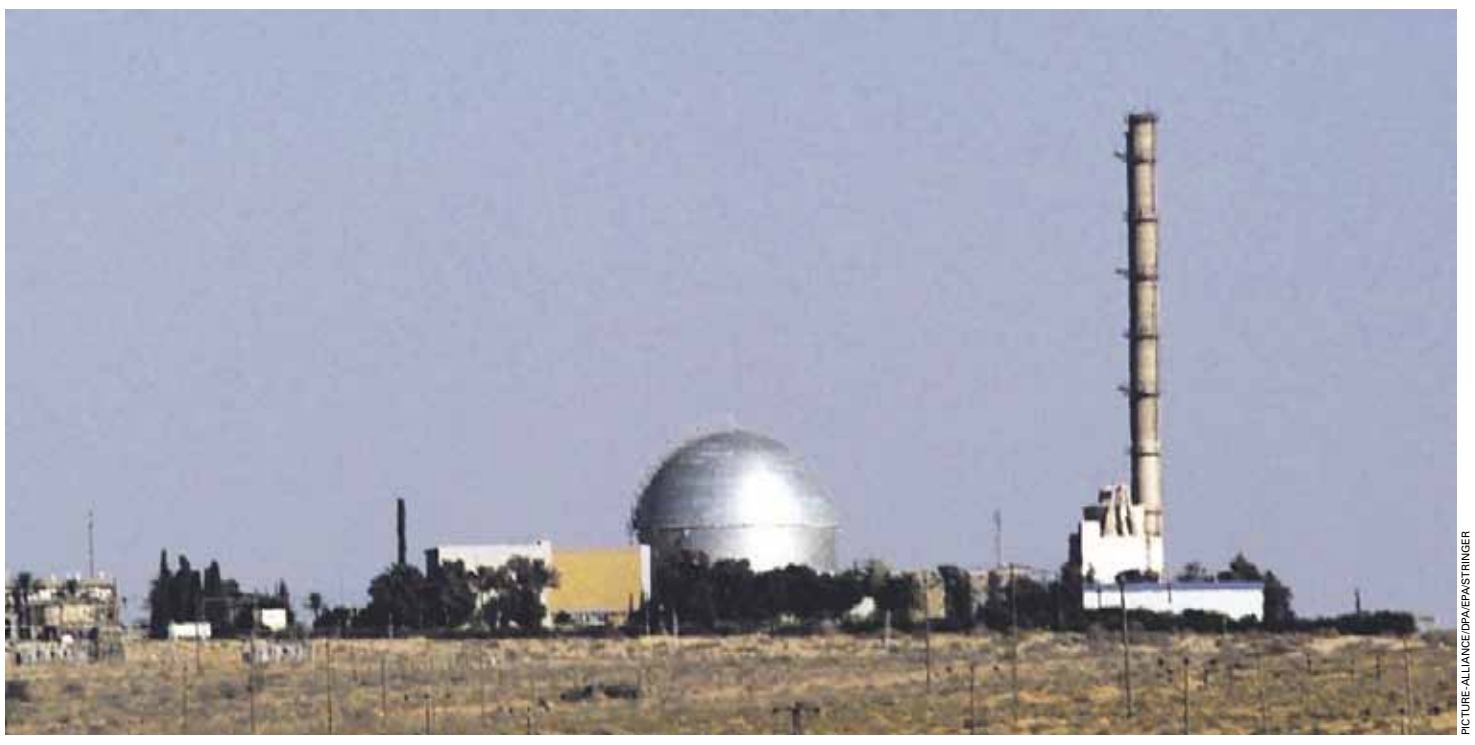
What should states do in this situation? First, instead of starting a verbal and physical cyber arms race in the era of Global Zero (the movement for the worldwide elimination of nuclear weapons), government officials and politicians are well advised to use the more measured language of cyber security or cyber crime when addressing the issue. Not only will this reduce the security dilemma, it also takes into account that not every cyber threat falls within the definition of national security.

Conventional response capabilities are of little use. The main problem with any cyber incident is the lack of clarity. Most perpetrators can and will remain unknown, if they want to. The difficulty of clearly identifying either the source or the possible attackers and their motives means that there is a high danger of retaliation against the wrong target or for the wrong reasons.

For more clarity, it is necessary to carefully investigate each incident; this means that it is always the law enforcement community that should act first – and not the defense community. Such a focus will also ensure that cyber defense is not understood as a military issue (only), but (mainly) as a civilian one. There is a need for close cooperation with the private sector, which owns most of a country's critical infrastructures nowadays, good computer forensic capabilities and international legal cooperation. One key issue for all countries alike is the harmonization of laws to facilitate the prosecution of cyber criminals.

Secondly, developments in the last couple of months have shown that it is high time that governments started talking earnestly about cyber peace to avoid a Wild West scenario in the Internet realm. The avenues currently available for arms control in this arena are primarily information exchange and norm-building, whereas attempts to prohibit the means of cyber war altogether or restricting the availability of cyber weapons are likely to fail.

However, these difficulties should not prevent the international community from pushing all countries to adopt responsible limits and self-restraint in the use of cyber weapons and from thinking about new and innovative ways to enhance protection of vital computer networks without inhibiting the public's ability to live and work with confidence on the Internet. The time is ripe for cyber diplomacy to strengthen an additional aspect of international cooperation in the digitalized world of the 21st century. ■



PICTURE-ALLIANCE/DPA/EPA/STRINGER

The Israeli Cyber Command is located near the country's nuclear center at Dimona. The computer worm Stuxnet's attack against the Iranian enrichment plant at Bushehr is reputed to have been engineered from this place in the Negev desert.

On Cyber War

Excerpts from the Strategic Concept of the North Atlantic Treaty Organization, adopted in Lisbon, November 19, 2010

Cyber attacks are becoming more frequent, more organized and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organized criminals, terrorist and/or extremist groups can each be the source of such attacks. […]

We will ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations.

Therefore, we will:

- develop further our ability to prevent, detect, defend against and recover from cyber attacks, including by using the NATO planning process to enhance and coordinate national cyber defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations;
- ensure that the Alliance is at the front edge in assessing the security impact of emerging technologies, and that military planning takes the potential threats into account.