11-15 APRIL 2011 • THE HAGUE • THE NETHERLANDS

WORLD FORESIGHT FORUM

Creating tomorrow

Issue Brief no 01

Dealing with **Cyber Security**: accept vulnerability

www.worldforesightforum.org

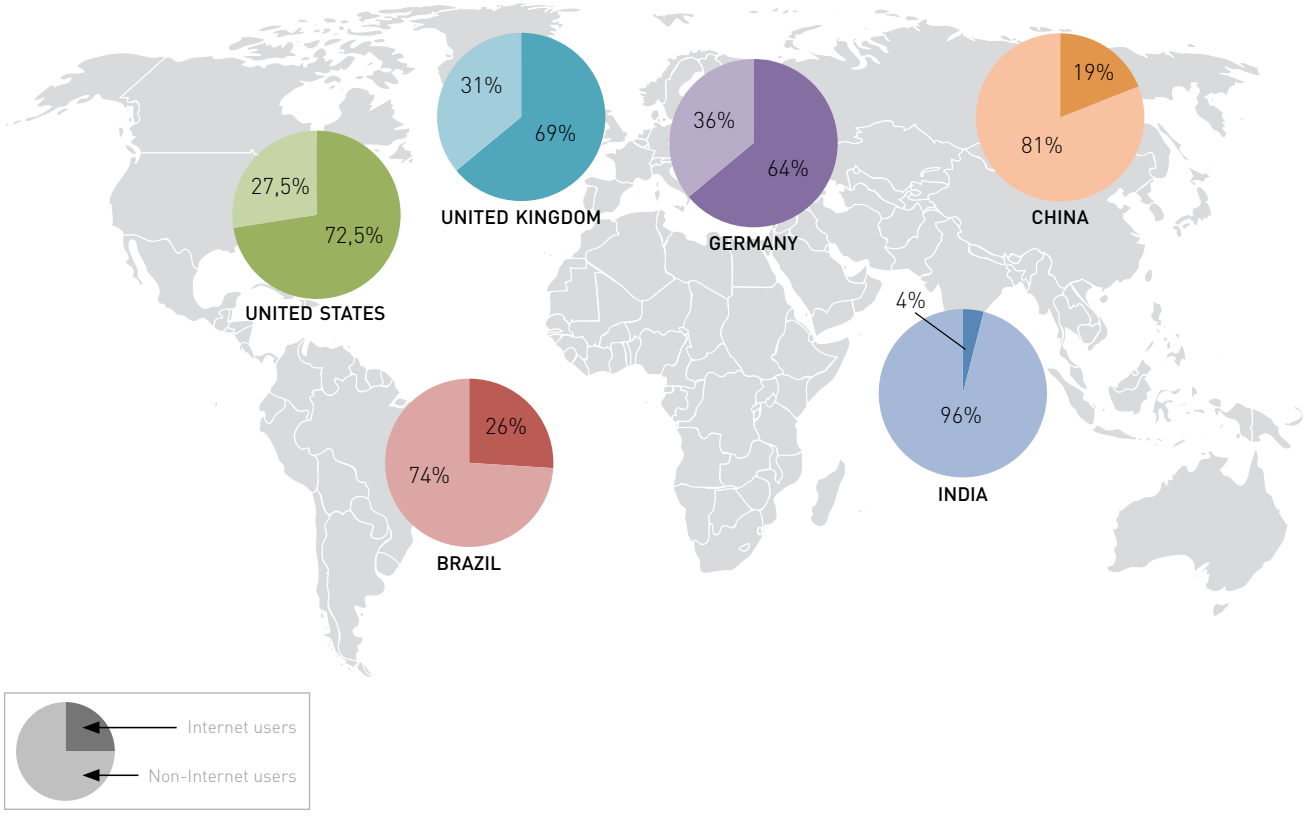
World Foresight Forum

Secure homelands for future generations

Introduction

By now, it is a truism to say that ICT technology is spreading rapidly. As growing economies like China, Brazil and India are nowhere near their full potential for ICT use, and even prominent western countries have not yet reached this limit (see figure 1), it is unlikely that this global trend is going to stagnate in the near future. It does, however, give rise to security challenges. The proliferation of ICT, especially in western societies, has increased dependence on digital systems. Information retrieval, online banking and digital process control systems are examples of processes that have been optimised through the use of ICT. The downside to these improvements is that they have made societies vulnerable to cyber attacks. Given the ongoing spread of ICT, this vulnerability is likely to further increase in the short to medium term along with the subsequent potential impact of cyber attacks. An ominous glimpse of what might lie ahead was provided by supporters of WikiLeaks-founder, Julian Assange. In retaliation for Assange's arrest, a group of his supporters launched Operation Payback, a series of cyber attacks on websites of the Swedish government, which had issued a warrant for Assange's arrest, and MasterCard and Visa, which refused to transfer donations to WikiLeaks.

THE EXPLODING INTERNET 2008



Data source: http://www.newscientist.com/gallery/mg20227061900-exploring-the-exploding-internet/8

Figure 1: The exploding internet

This Issue Brief considers the most disturbing cyber threats, namely those coming from actors who attempt to cause social disruption by launching attacks on ICT infrastructure. The actors may vary from hackers to cyber-activists and from terrorists to even state actors. The instinctive reaction to this threat might well be to increase the security of all ICT-dependent functions, but individuals, organisations, businesses and governments would be wise to accept vulnerability to some extent and focus on the resilience and recovery of their ICT-infrastructures. Given the anonymity of cyber attackers, that may be the only viable option.

As full security of ICT systems is impossible, cyber security policies should no longer focus predominantly on protective measures, but should put more effort into restoring a state of normalcy after an attack has taken place.

Cyber attacks and 'hacktivism'

Cyber attacks can be launched for many reasons. Some cyber attacks serve propaganda purposes, like the attacks on Georgian media websites during the 2008 Ossetia War, when the usual contents of these websites were replaced with pictures comparing Georgian President Saakashvili to Hitler (see box 1). It is also possible that cyber attacks are intended to cause social disruption, for instance by paralyzing urban or national electricity grids or water supplies. In a purely military context, a cyber attack can affect the enemy's capacity to respond to a conventional attack, for example in the event of an attack against the enemy's communication system or reconnaissance equipment. The potential reasons as well as the potential perpetrators of cyber attacks are manifold.

Although cyber attacks are notoriously difficult to trace, several security services have mentioned China as one of the main culprits. The Dutch and the German security services did so in their annual reports and the British security service has warned top executives in the private sector about the threat of Chinese cyber attacks. However, the threat to cyber security does not emanate

CYBER ATTACKS

- In April 2007, **Estonia** suffered a wave of 'denial-of-service' attacks, probably in retaliation for its intention to remove a Russian war monument. The websites of several media, government offices and banks were shut down. The attacks are widely believed to have been launched from Russia, but involvement of the Russian government has never been proven.

- In September 2010, the **Stuxnet worm** was used to sabotage one of Iran's nuclear enrichment facilities. The impact is unclear, but Iranian officials allegedly admitted "serious damage that caused damage and disablement". The origins of the Stuxnet worm, which experts consider a very advanced piece of software, remain unclear.

- In 2008, shortly before the **Georgian** invasion in South Ossetia, several Georgian media and government offices were struck by a wave of 'denial of service' attacks, some of which mainly served propagandistic purposes, as they took over the sites to show materials that drew parallels between Georgian president Saakashvili and Adolf Hitler (see illustration).

Box 1: Examples of cyber attacks

World Foresight Forum

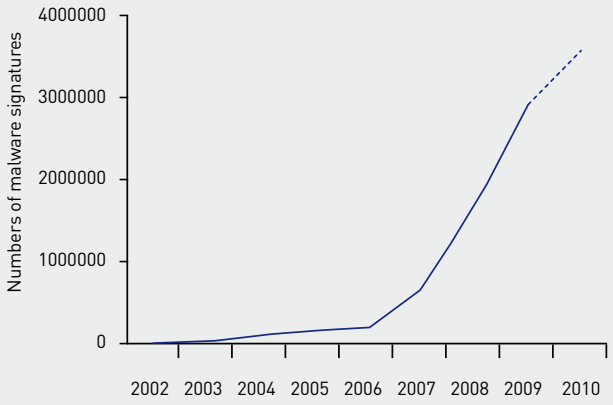
Secure homelands for future generations

'HACKTIVISM'

- On May Day 2010, tens of thousands protesters in Greece displayed their frustration about austerity measures. The demonstrations turned violent, with groups clashing with police and youth throwing stones, chanting "people don't bow down, it's time again for revolution".
- During the Israeli invasion in Gaza in early 2009, hacktivists from both sides engaged in 'denial-of-service' attacks, website defacings and efforts to shut down facebook groups, primarily in an attempt to discredit the opponent and win the propaganda war.
- During its 2009 edition, the Melbourne International Film Festival was forced to shut down its website after Chinese hacktivists had launched a series of 'denial-of service' attacks. The reason was that the festival would show a movie which the hackers considered anti-Chinese. Festival-related information on the website was replaced by the Chinese flag and slogans criticising the controversial filmmaker.

Box 2: Examples of 'hacktivism'

NEW MALWARE SIGNATURES AND THE FORECASTED TREND



Data source: Symantec Global Internet Security Threat Reports

Figure 2: Numbers of new malware signatures per year

from state actors alone. Non-state actors may want to attack ICT infrastructure as well. In some cases, the attack is not intended to cause social disruption but to propagate a political cause. This latter phenomenon has been labelled 'hacktivism' (see box 2). So far, non-state actors have not caused large-scale disruption, but there is no guarantee that they will not do so in the future. The number of malware signatures has grown dramatically over the last couple of years, indicating an increasing willingness to engage in actions to break into or otherwise disturb ICT-systems (see figure 2).

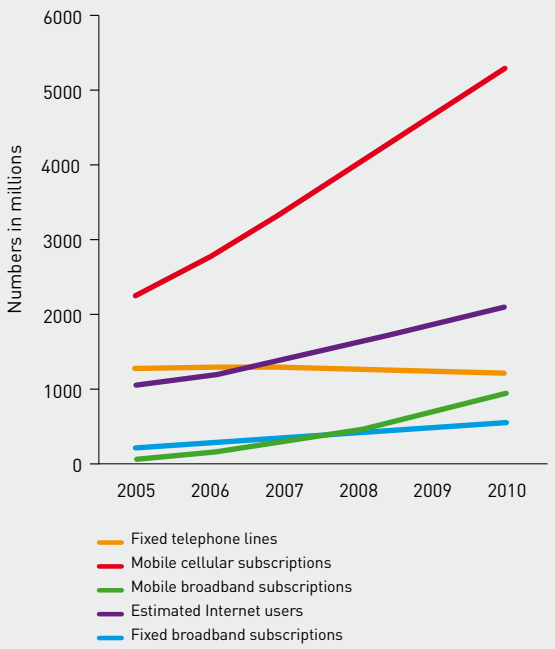
Impact of cyber attacks

As societies continue to become more dependent on ICT, cyber attacks will become an increasingly viable and strategically interesting option, for both state and non-state actors. Figure 3 shows a strong upward trend in the proliferation of ICT, and there is little reason to assume that this trend will be reversed any time soon. For instance, an increasing number of public and private services are controlled by ICT. Water, electricity, banking and aviation are just a few examples of goods and services that can only be provided when their ICT infrastructures are up and running. What exacerbates the vulnerability is that many ICT systems depend on each other. A cyber attack can thus create a 'domino effect', where the disruption of one system is the result of the disruption of another. The potential impact of cyber attacks is, therefore, growing and can be achieved at relatively little cost to the perpetrator.

ICT vulnerability

The ICT domain is rife with vulnerabilities to cyber attacks. As a result, it is unrealistic to assume that ICT networks can guarantee the deflection of all attempted illicit penetrations. There are three main reasons for

KEY GLOBAL TELECOM INDICATORS FOR THE WORLD 2005-2010



Data source: International Telecommunication Union
http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html

Figure 3: Key Global Telecom Indicators

this. First, hackers can easily operate anonymously and their actions are hard to trace, thereby lowering the barrier to engage in malevolent cyber activities. For example, hackers may use proxy networks to conceal their IP addresses. This is not hard to do and even casual users sometimes use these networks to hide or reroute their traffic via different servers. A benign application of these networks may be to circumvent online censorship, but hackers use the networks to hide their tracks. Secondly, ICT networks cannot be anything other than complex systems of interdependencies. There are so many elements that can be attacked that it is virtually impossible to fully rid systems of all vulnerabilities that may jeopardize security. This is further complicated by new technologies which may render previously secure parts of systems vulnerable. Lastly, a security problem that is often overlooked arises during production, even before systems go online. As a cost-cutting exercise, many ICT components are manufactured abroad, which leaves the integrity of components open to corruption through the introduction of 'backdoors' in the hardware that allow hackers to covertly penetrate systems despite the presence of the latest security measures. ICT security therefore requires either indigenous ICT component production or an integrity verification system.

Cyber security and national security

With a growing number of salient cyber attacks and increasing potential impact, the need to address the security of the ICT infrastructure has not escaped policy makers. In several countries, this growing prominence has prompted policy makers to include the protection of ICT infrastructure in their national security strategies, treating them on a par with more 'established' threats like terrorism (see figure 4). Also, some countries, such as Australia, the US, the UK and Canada, have adopted cyber security strategies (see figure 5).

Understandably, these strategies stress various types of protective measures. First, they engage in what one could call the last line of defense, that is, measures to protect objects against attacks. With regard to cyber security, one could think of installing firewall systems on a network, either as software or as hardware. However, given the many vulnerabilities of ICT systems, this type of strategy is likely to be insufficient for the three reasons mentioned in the previous paragraph. Therefore, the strategies also include elements of a second type of protective measures, the so-called defense-in-depth strategy designed not to ward off an attacker, but rather to delay and disrupt cyber attacks, and to increase the costs of an attack.

World Foresight Forum

Secure homelands for future generations

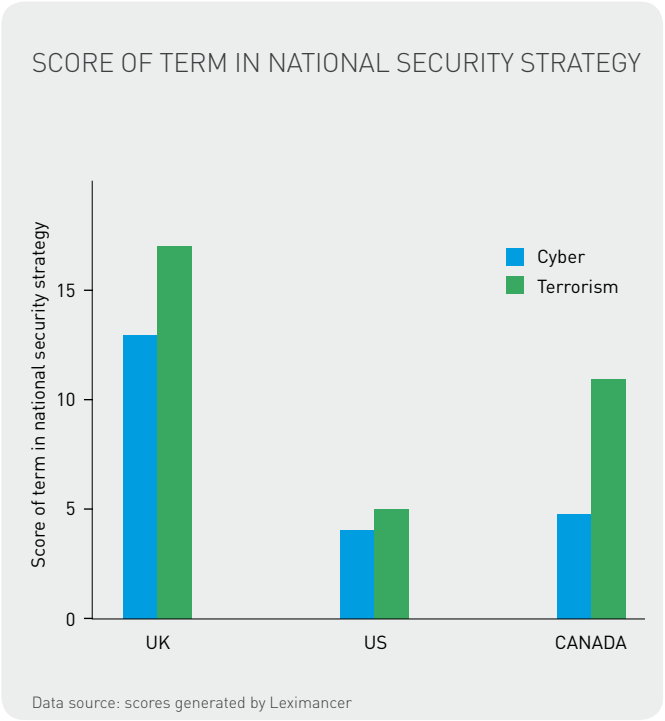


Figure 4: Cyber issues and terrorism in three national security strategies

Figure 5: Cover pages of the Australian, Canadian, British and US cyber security strategies

By adding multiple layers of defense, with each new layer providing a unique obstacle, cyber defense gains time and is better able to detect, fend off or mitigate a cyber attack. This defense-in-depth strategy encompasses more than mere technical solutions and may be considered a process rather than a product, such as a firewall. It also includes raising awareness and the training of personnel and users of networks, something that is addressed in all four strategies.

Given the nature of the cyber security threat as discussed in the previous section, it is doubtful, however, whether these approaches will suffice. The anonymity of the cyber attacker especially has important implications since, with anonymity more or less guaranteed, there is little point in focusing on deterrence or retaliation. Both deterrence, one of the pillars of the US Comprehensive National Cybersecurity Initiative (CSNI), and retaliation depend on the ability to identify and locate the enemy, which is extremely difficult in the case of a cyber attack. For instance, laws against cyber attacks will not deter cyber attackers who know that they cannot be found. This is not to say that no laws against cyber attacks should be introduced, but this approach should not be the main thrust of a cyber security strategy. Also, the CSNI emphasizes threat detection and cyber counterintelligence. Of course, actions along these lines are useful in learning about the methods used by cyber attackers, but it should be noted that here the anonymity of cyber attackers is again an inhibiting factor. As it is impossible to monitor all potential cyber attackers, the nature of the next cyber attack is consequently bound to remain uncertain. This being the case, it is difficult to take adequately informed security measures. Therefore, more emphasis should be put on post-attack recovery,

an approach that none of the strategies, with the possible exception of the British one, explicitly endorses.

The new approach

The Australian and the British cyber security strategies recognize, at least more so than the CNSI and the Canadian strategy, that the nature of the threats to cyber security calls for a new type of strategic thinking about the means to counter them. The anonymity of the attackers makes strategic concepts like deterrence and retaliation difficult to implement accurately. Also, security measures may not suffice in a situation where little is known about the nature of the cyber attack. In the words of the Australian Cyber Security Strategy: "The inherent characteristics of a borderless, lightly regulated and largely anonymous online environment make it impossible to prevent all security incidents from occurring." In spite of the merits of measures to protect ICT systems against cyber attacks, policy makers therefore need to accept a certain level of vulnerability and redirect their focus to recovery and resilience, the ability to restore a state of normalcy after disruption. With recovery and resilience as the core principles, the primary cyber security objective is not about deflecting all cyber attacks, but rather about effectively mitigating the impact and quickly restoring the original situation. A recovery-and-resilience approach extends beyond technical measures alone and should also include measures to train staff and users of vital ICT networks, develop a joint public-private response capability, facilitate rapid public-private information exchange, allocate a central communication point, and inform and involve the public.

This publication is part of a series of WFF Issue Briefs that offer background information on themes to be addressed at the World Foresight Forum. The Issue Briefs aim to inform and stimulate the debate on global challenges. The views and opinions expressed here are those of the authors and do not necessarily express the official views of the WFF or any of its speakers or sponsors.

World Foresight Forum is an initiative of

Authors: Islam Qasem, Teun van Dongen, Marjolein de Ridder

World Foresight Forum (WFF)
Lange Voorhout 16
2514 EE The Hague
The Netherlands

T +31 70 363 6503
F +31 84 215 3165

info@worldforesightforum.org
www.worldforesightforum.org