Invisible Enemies

The new magnitude of cyberspace threats

Henning Wegener | **Digital technologies have revolutionized our world—and added a host of immense security challenges. The stability and security of digital networks and our privacy face serious threats by attack systems with immense sophistication and power, yet the scale of the dangers receive far too little attention.**

It hardly needs to be argued that the expansion of digital information and communication technologies (ICT) into every aspect of civilized life has ushered in a new era. The stability and security of digital systems and networks, confidence in their reliability and integrity, and the protection of privacy have become vitally important. Information security thus needs to be ranked as an overarching societal challenge of universal proportion, given that digital technologies negate distance and frontiers, as well as time.

The benefits of the digital age are clear. But the digital planet also has its dark, even sinister, side. All digital devices and the nets connecting them are extremely vulnerable as a matter of technical principle, and open to invisible misuse. These vulnerabilities are growing exponentially. While there are more and more benefits from new technologies, the accompanying risks and damages grow disproportionately: More good comes with even more bad. And we may well be nearing a true shift in the quality of the threat. There are many who argue that faceed with the ubiquity of digital systems and their tremendous fragility, we may not be able to win the battle against an ever-more potent cybercrime attack system with its immense sophistication and power. In the age-old struggle between attacker and defender, here again the attackers appear to have the advantage, since, besides often being better "armed," they can freely choose the intensity of the attack and the target, unfettered by geographical constraints.

Awareness has not kept up with this new array of threats. Despite a host of activities and counter-strategies by governments, industry—including a highly developed security industry—and international organizations, the threats in cyberspace are trivialized despite the rising damages.

To start, a definitional clarification

appears in order. At its core, cybercrime is the direct interference in the operation of data processing and storage systems through illegal access, data theft or manipulation, or through disruption, destruction or misuse of the systems themselves. These are crimes against the integrity, authenticity, availability or confidentiality of digital systems and their data, as also defined in the Council of Europe's trail-blazing Convention of Cybercrime (2001). This is different from the equally important crime of using the Internet (and other digital means) to project illegal content (child pornography, infringement of copyright, advocacy of terrorism, fraudulent offers of all kinds, etc.). As the large part of content-related cyber delinquency is subject to normal national and international sanctions, this analysis predominantly relates to the first area of cybercrime: the technical manipulation of digital systems and the data they handle.

The new dimension of the threat is, in the first place, a number game. Presently there are more than 1.5 billion conventional Internet-capable computers in operation, a growing percentage of them broadband connected (in some countries more than 80 %). Broadband access is indispensable for all digital management functions and data transfers. These computers are an important part of the endangered digital environment, but all other varieties of digital devices containing microprocessors for handling digital data are equally at risk. These include, in particular, microprocessors in embedded systems; mobile systems for mobile telephones and an array of hand-held devices; and the omnipresent sensors such as RFID (radio frequency identification devices). The number of units is easily in the tens of billions. The developments underway, conventionally labeled "next generation," demonstrate where this journey leads us in terms of quantity: ultra-miniaturization of digital circuits, massive use of multicore processors, increased use of fiber, huge volumes of data traffic reaching a new order of magnitude, development of new "smart" devices, maturing of quantum computing research, and ubiquity of new miniaturized computing elements leading to different and novel structures of processing configurations in digital nets (including "artificial neural nets"). Embedded systems, biometry, the steady progress towards an "Internet of Things" with miniature computers inserted in cloth or eyeglass frames, the development of minute computers with self-organizing potential, able to communicate autonomously with other digital devices, new human mind-machine communication,—all these developments contribute to the explosive growth of digital actors and to the exponential growth curve of interconnectivities, which automatically spell a parallel increase in vulnerabilities.

The new dimension of the threat is, in the first place, a number game.

Added to these quantitative developments are the phenomena of migration and convergence. The differentiation between the various digital operating modes is vanishing. Fixed line telephone networks are giving way to wireless communication and to the Internet (Voice over IP). Computing processes and the mass storage of data are moving from individual and business computers to huge external data centers (server farms, "grid-computing", "cloud computing") with thousands of servers and storage capacity at petabyte level. A momentous, revolutionary, and probably irreversible shift is underway that concentrates computing, software management, and data storage in distant, undisclosed locations, without any transparency in their procedures and security measures, relegating traditional computers to mere portals of access, and depriving conventional firewalls of their function. The result is a huge integrated network structure with a universe of connectivities and vulnerabilities that defies quantification. It includes a myriad of important components totally open to attack.

Huge cybercrime syndicates have supplanted a generation of youthful, playful hackers.

New Techniques, New Threats

Virus attacks accompanied the earliest phases of the computer age during the second half of the 20th century, often on a massive scale; but those attacks were quickly countered by antivirus software. But that romantic age is irretrievably gone. The new forms of attack are best understood through their perpetrators. Huge cybercrime syndicates, a new form of organized crime, have supplanted a generation of youthful, playful hackers. Highly professional and with unlimited technical and financial resources, they specialize in making money through fraudulent cyber operations. They are concentrated in a few—KNOWN?—countries, but channel their attacks through other countries—principally the United States—to hide their identity ("station-hopping"), and also use inconspicuous individual Internet users for specific purposes such as money laundering. These consortia have accumulated comprehensive data bases of e-mail addresses, enabling them to send huge packages of spam—a profitable undertaking. Today, an estimated 80–90 % of e-mail traffic worldwide is spam, unnoticed in its full extent by individual users because of the spam filters put in place by their Internet service providers (ISP). Spam messages are more than a nuisance: they are effective vehicles for virus infections and other damaging software ("malware"),—not only in e-mail attachments, which one would be well-advised to not open, but increasingly also through the main spam text. Ten years ago, the conventional estimate was that there were around 40,000 virus variants circulating; in 2008 the cyber security company, Panda, calculated this figure to be 13 million. In all cases of malware, protection programs only neutralize known versions; but new attackers constantly develop new variants, often with superior technical proficiency and breathtaking speed, so that the defenders have to address new vulnerabilities without respite, a breathless race.

Probably the most menacing new development is the emergence of botnets. The term denotes the implantation of a dormant virus, unnoticed by the Internet user, which the attacker can activate at any time ("trojans").

They transform the infected computers into "zombies", robots which execute orders, and, if available in sufficient numbers, allow the criminal manager ("bot herder" or "bot master") to launch massive hostile operations. Big botnets are organized hierarchically, almost militarily. Botnet infection is estimated in some countries to reach 60 % of all computers. Some variants of botnet software are able to function autonomously, recruiting further computers into their network. The botnet software spies on the infected Internet user, including private passwords. In this way, the herder can access bank accounts, steal business figures or clients' data, production planning and design, and falsify data. Data espionage increasingly enables identity theft, by which the perpetrator can substitute himself for the person spied upon and act on his account and to the victim's detriment. Via botnets it is possible to interfere in the process functions of the infected computer (logic bombs), and to destroy or to alter the stored data. No less grave is the ability of botnets, simultaneously "activating" a large number of zombie computers, to saturate and block targeted e-mail addresses, or even durably damage their connections ("distributed denial of service"—DDoS). This can cause, not only entire enterprises or business branches to stall, but also halt essential national infrastructures (governments, electricity supply, steering computers in the banking system, aviation and railway traffic, the command posts of dams, the underlying ITC infrastructure itself, etc.) with extraordinarily harmful effects. The same is true, alarmingly, for national defense installations. Botnets triple threat of data espionage, especially in the industrial and defense sector, logic bombs, and DDoS, is ominous indeed.

The botnets set up by organized criminals attain ever more menacing levels. The biggest net discovered so far is estimated to have enslaved 1.5m computers. The newest threat—against which no counter strategies have yet been found—, the botnet Conficker, is said to be able to command five million computers in 122 countries.

Other routinely practiced methods for criminal gain, both through botnets or not, are phishing and pharming. Both are ways of rerouting of computers to fraudulent imitations of bank sites designed to obtain passwords, credit card numbers, etc. which allow the subsequent pillaging of bank accounts (about 60 % of economic crime is in this category). The total annual economic loss through cybercrime is estimated to reach tens to hundreds of billions; a reliable estimation calculates 180 billion euro. Exact numbers are impossible to estimate, as enterprises, especially banks, often cover damages quietly themselves to protect business and customer confidence.

Botnets transform the infected computers into zombies.

More than Money

The huge profits available to organized crime from digital economic delinquency are only part of the danger. More important are the new possibilities in the area of cyber conflict. The dimension of the new botnets enable coordinated simultaneous attacks against the economic system, critical national infrastructures and the national defense structure of a country —all of them very interdependent—, thus stalling all vital societal functions in a matter of seconds. Recent events in Estonia and Georgia provide a foretaste of the applicable techniques and possible results. There can be no doubt that the technical prerequisites for a digital Pearl Harbour—and more—now exist. Without dwelling extensively on cyberwar scenarios one must underline that apart from a massive blockade of ITC nets—and all defense ministries today use the civilian nets in addition to protected infranets which are also not immune to cyber attacks—assaults could include espionage into defense planning and intelligence, the manipulation of battlefield information, interference in command lines, and the proper functioning of weapon systems.

There can be no doubt that the technical prerequisites for a digital Pearl Harbour—and more—now exist.

The direct profit-oriented activities of the bot-herders are only part of their business model. The latest generation of malware hints at the vulnerabilities of conventional software, and instructions for the theft of passwords or credit card numbers can be bought online. Huge lists of e-mail addresses are also for sale. Crime syndicates offer to sell, or lease hourly, cyber attack services, making it possible for other criminal actors, especially terrorists—or perhaps hostile governments—to hide behind such unholy alliances without any risk of identification. Here again, the Estonian case offers more than food for thought. In the face of such criminal creativity the borders between cybercrime, cyberterrorism, and cyberwar blur.

Most governments are taking precautions in their defense sector. A policy of prevention—protection of ICT infrastructure, redundancies, cyberwar countermeasures—is legitimate. Problematic, on the contrary, is that some 140 countries, including all major powers, have also equipped themselves with offensive information technology and include cyber attack options in their military planning. A clear distinction between digital attack and defense technology is difficult; intent and strategic planning, however, allow for distinctions.

If information security and work on effective countermeasures should be commensurate with the exponential growth of the threat, then current efforts are clearly still inefficient—despite considerable investments and remarkable advances by the security industry, an abundant literature, and authoritative calls for a “global culture of cyber security. Major challenges lie ahead for governments both collectively (for example in creating a seamless global penal system for cybercrimes[1]) and individually (including more effective and better coordinated

[1] See the Council of Europe Convention on Cybercrime, and the “ITU Toolkit for Cybercrime Legislation,” http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

cyber defense organization).[2]

We are in dire need of a modern international legal framework for dealing with military uses of ICT (cyberwar and cyber defense). It is possible to deduce some general standards from extant international treaty law and the overarching principles contained in some UN General Assembly Resolution[3] on aggression and intervention. However, the task of adapting international law to the requirements of the digital age has hardly been tackled. Any success at drafting digital international law would presuppose an authoritative reinterpretation of the UN Charter (and of the NATO Treaty) with respect to terms such as "armed attack", "territorial integrity," and "national sovereignty." We also need a definition of "information weapons" and their offensive use, just as the development of operational standards for the application of Chapter VII of the Charter, or collective countermeasures under the NATO Treaty. In this context we should consider prohibiting the use of cyber weapons, despite the difficulty of delineation between offensive and defensive deployment and use of ICT and the problem of the feasibility of sanctions.

Beyond these momentous tasks, there is an overarching challenge. As with the seas and outer space, we need a comprehensive concept of cyberspace. Codification of the seas was possible with the UN Convention of the Law of the Sea (1982), and for outer space a regime of basic legal standards is in the making. A similar regime for the digital sphere, an international "Law of Cyberspace"[4] would enable a more conclusive and logical treatment of cyber conflict and the adoption of a universally valid Cyber Code of Conduct. We can hope that this may bring us closer to a world dominated not by threat of cyberattacks and massive destabilization, but the normalcy of a cyberpeace.

(TEMP) The task of adapting international law to the requirements of the digital age has hardly been tackled.

[2] A comprehensive strategy such as needed cannot be developed here in more detail; see a recent compilation of the priority tasks to focus on: "Top Cyber Security Problems That Need Resolution", World Federation of Scientists, Geneva, May 2009,http://www.unibw.de/infosecur/documents/published_documents_cyber_security_problems.

[3] e.g. "Definition of Aggression," Res. 3314 (XXIX), "Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations," Res. 2625 (XXV).

[4] Cf. *Permanent Monitoring Panel on Information Security, World Federation of Scientists* Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar, 2003.