diploweb.com La revue géopolitique
ISSN : 2111-4307

Can deterrence work in cyberspace ?

dimanche 13 juin 2010,par Charles BWELE

Citer cet article / To cite this version :
Charles BWELE, **Can deterrence work in cyberspace ?**, *Diploweb.com : la revue géopolitique, 13 juin 2010.*

How can a state or organisation be prevented from launching a cyberattack against the vital systems of a nation ? How can they be deterred from this and how can the proliferation of cybernetic weapons be monitored ? Charles Bwele gives his thoughts on cyberdeterrence.

As part of its strategy of geopolitical synergy, *diploweb.com* is pleased to present this article, which first appeared in *Revue Défense Nationale*, June 2010.

HOW CAN a state, an individual or a non-state organization be prevented from launching a cyberattack against governmental data networks or vital infrastructure ? Does an online non-aggression pact or control of cybernetic weapons make any sense when a laptop computer or a mobile phone can become a weapon ?

A very real virtual threat

Since the spring of 2010 the United States and Russia, followed by six other countries, have been attempting to negotiate a treaty on Internet security and the restriction of the military use of the Internet. A significant divergence became apparent immediately : Washington is insisting on notions of 'IT security' and 'cyberwar' while Moscow favours a wider concept of 'information security'. For the Americans, cybercriminality and cyberespionage constitute the major problems ; for the Russians, the protection of government IT architectures remains the priority.

Beyond the pious hopes and behind-the-scenes manoeuvres, this 'Cold War' type of approach to security, partly justified but deeply mistaken, is the product of leaders who have come lately to information technology, rather than being born to it. Hence their great difficulty in understanding the finer points of the emerging paradigm of cybersecurity.

In addition, any concept of cybersecurity must include the protection of vital infrastructure (electricity, gas, fuel, transport, telecommunications, emergency networks, etc.), which depend almost entirely on control and communication systems termed Supervisory Control and Data Acquisition (SCADA) systems, or more simply, 'telesurveillance and data acquisition'.

A few decades earlier, when the Internet was merely a discreet military and scientific application, SCADA systems were based on engineers' pipe dreams, operating over closed circuits via radio transmissions, satellite links, ISDN, power lines and proprietary networks, and had no need for integrated cybersecurity measures. Gradually, SCADA systems were connected, directly or indirectly, to the wire- or radio-linked Internet in order to reduce the communication costs involved in their daily use by the water, electricity, gas and fuel distribution companies.

Like the Internet upon which they depend, these systems are often victims of their intrinsic complexity rather than any 'hacking'. Also, updating old SCADA systems in accordance with cybersecurity norms still in their infancy is a complicated, onerous and sometimes risky task. The recent brief power cut in your neighbourhood was possibly due to a tiny updating error in a SCADA.

Fortunately, SCADA systems are increasingly connected to the Internet by highly secure modems, routers, applications and protocols. Moreover, let us not panic about a technological apocalypse : these technologies embody safety parameters in case of alert or events dangerous for the ‘real world’, even in the case of cyberpiracy. Finally, too many cybersecurity scenarios neglect the human factor capable of reacting, improvising and especially manually intervening in the event of an emergency. As equipment, IT and network key points of vital infrastructure, and hence important in daily life and the economy, SCADA systems constitute potential targets.

Unfortunately, the spectacular cyberpiracy of a hydroelectric power station in Brazil highlighted the danger of malware to vital infrastructure. A dozen Brazilian cities and their 60 million inhabitants were deprived of public transport, traffic lights, telecommunications and even lifts for three days. Service stations, banks, shopping centres and industrial sites by the thousand were completely paralysed or greatly hampered. More than enough to concern an emerging country organizing the World Cup in 2014 and the Olympic Games in 2016 ; or to scare an America or Europe increasingly dependent on data networks.

This incident dramatically highlighted the possibility of a sophisticated cyberattack against vital infrastructure, with its quota of damage and disruption, temporary perhaps but not greatly different from that caused by aerial bombardment. Such a scenario in a European country would certainly have repercussions for neighbouring countries in view of the regional integration there and continent-wide extension of vital infrastructure.

For non-state malicious organizations (criminal, cybercriminal or terrorist), a cyberattack against some vital infrastructure would constitute an instrument of terror or reprisal amounting to a ‘weapon of mass nuisance’. For conflict states, such an act would probably be included in a large-scale military operation. For an isolated hacker or a hacker group, it would be a great technical exploit. It is clear that diversity and anonymity are also features of cyberwarfare.

Online reconnaissance

The Internet is swarming with activity worthy of a novel by Tom Clancy or John Le Carré. As well as cybercriminals from the four corners of the earth, states of all kinds unceasingly ‘penetrate, probe, scan and search’ the IT networks and vital infrastructure of their counterparts, whether they be allies, neutral or enemies. Their objectives are :

. to extend their policy of industrial and military espionage on the net ;

. to detect critical weaknesses within SCADA systems ;

. to find out more about their own vulnerabilities by detecting those elsewhere.

This does not only involve cyberespionage but also online technical documentation.

To a certain extent these intrusions, which do not amount to cyberattacks, are to cyberespionage what the camera is to industrial espionage : a valuable intelligence tool with the additional benefit of asymmetry and stealth by virtue of its purely electronic nature. Also,

the risk of a diplomatic or political incident is negligible and no official complaint will be made after the discovery of malware within a sensitive server or a SCADA system.

Governments and commercial enterprises of all types rarely advertise their vulnerabilities when they are secretly exploited by an identified intrusion. The bad publicity which would result would upset clients, suppliers, partners and even shareholders. In addition, it would take a clever company or state to establish incontestable proof of the involvement of another. In cyberespionage, as in cyberwarfare, organizations as far as possible avoid pressing the button or pulling the trigger themselves. They prefer to resort to hackers gifted in the computer arts of camouflage and deception.

Anyone who can penetrate to the heart of a piece of vital infrastructure can equally plant undetectable 'logic bombs' [1] which, once set off, would cause severe domino effects in various segments of an electricity distribution system or a telecommunications network. Hence the need to understand how and why the principles of nuclear deterrence and arms control are not well adapted to cybersecurity threats.

Towards a proliferation of cyberweapons ?

A cyberweapon is essentially based on computer science. Short of changing the laws of physics, mathematics and electronics, burning the scientific literature, imprisoning science and technology professors along with their disciples the programmers, dismantling and banning the IT industry and amending in depth the law (international, public, private, commercial, data, etc.), cyberweapons will continue to proliferate.

A cyberweapon is simply a computer or a connected mobile phone and a series of algorithms (software, malware, spyware etc.). There is no need for specialized or banned equipment, production or enrichment plants, complex logistics, colossal financial resources or scarce skills to mass produce them.

A cyberweapon hardly needs a particular launch site ; a fixed or portable computer, a mobile telephone, an Internet site, a search engine, a social network, a physical or virtual server or a 'data cloud' all constitute launch platforms.

A cyberweapon can be designed or used anywhere, by anyone, with or without a motive, such as a hacker, political or religious extremist, terrorist, cybercriminal, discontented ex-employee, competitor, conflict state, 'madman', etc.

A cyberweapon leaves very little time for anticipation, prevention, detection or reaction due to the electronic speed of action conferred by its vectors, namely the IT architectures and data transmission networks. How can we clearly assess the situation and mount a response when the electricity is cut off ?

The origin and workings of a cyberweapon are increasingly difficult to identify and counter. Whether on or outside national territory, the cybercriminal always spreads his activities over a multitude of computers located in several countries in order to increase his operational effectiveness and complicate the task of computer experts trying to repair the damage.

Cyberwar, cyberespionage and cybercriminality use identical tools and operating modes. This

poses an insoluble problem of attribution of the intrusion or attack to an individual, a state or a non-state culprit. Stealthy software such as the botnet [2] or the rootkit [3] permit hundreds of computers to be turned into zombies, including the one on your table or your lap, and make them vectors of a malicious intrusion or a wider-ranging attack.

By virtue of their constant development, information and communication technologies are concepts in perpetual gestation. Threats which today belong to the realms of futurology are rapidly becoming tomorrow's reality. In less than a decade, the Internet of things, or IOT, which attributes an Internet address or an intelligent interface to a physical object, will perhaps distribute logic bombs timed to go off only at a programmed date or under certain conditions.

The proliferation of cyberweapons is not behind but in front of us. If the nuclear weapon was one of the ultimate symbols of the industrial era, cyberweapons are the direct descendants of the information era. Even inactive, the first possesses a perceptible physical reality and measurable effects, while the second remains—in spite of its impact on the real world—fundamentally immaterial and intangible : in a word, virtual.

So, how are we to define an act of cyberwar ? How do we identify its perpetrators ? Can we take reprisals against a state for misdeeds committed by some of its citizens ? What rules of engagement must those who police the code respect ? Where does the battlefield begin and end ? How do we establish and apply a cybernetic non-proliferation treaty ? What legal framework would govern the inspections of a putative 'International Agency Against the Proliferation of Cyberweapons ? What technical and human resources would be available to it ? However states prove their credentials in abstaining from the use of cyberweapons, what about their population ? How can hackers be discouraged from attacking a government server or a piece of vital infrastructure ?

In view of the pervasiveness [4] of protocols and the growing interconnection of information systems, companies, industries and hence economies, governments must take these questions seriously before they charge into online reprisals and cause enormous collateral damage.

In spite of the complexity of this cybersecurity issue, a detour through history and strategy will provide food for thought and will help to clarify things.

Resilience as a deterrent

During the Cold War, deterrence consisted in persuading the opposing camp not to launch a conventional or nuclear attack on pain of becoming the victim of an extremely costly riposte in human and material terms. In addition, with the immense nuclear arsenals available to NATO and the Warsaw Pact, the risk of mutual assured destruction (MAD) avoided any reheating of the Cold War. In cyberspace, potential or real aggressors are much more numerous and less reliable than was the case for nuclear deterrence : terrorist networks, hacker movements, cybercriminal organizations and isolated hackers have nothing to stop them resorting to weapons of mass nuisance or 'cybotage'. Cyberwar is also an individual affair ; the type of open and participative cyberwar exploited by Russia against Georgia in the summer of 2008 is a perfect example of this.

All the same, why not invert our perspectives ? If nuclear deterrence ‘intimidates’ enemy offensive action upstream, cyberdeterrence would neutralize enemy offensive action as much as possible downstream thanks to three elements :

. a solid and skilful combination of cybersecurity perimeters protecting information networks and infrastructure : electricity, water, gas, telecommunications, transport, health, finance, government, police, armed forces, etc ;

. improved and permanent redundancy of these information networks and vital infrastructure, which would reduce or eliminate the domino effects caused by cyberattacks ;

. surveillance and the action of human operators in the cybersecurity loop, which would have sufficient margins to analyse the situation closely and adopt protection and redundancy according to their evaluation of the risks and damage.

To some extent, ‘cyberdeterrence’ would rest primarily on increased resilience in strategic information networks and vital infrastructure. In parallel, this would demonstrate to would-be attackers that their actions would have only limited or brief consequences. It goes without saying that this would be a huge programme.

Revue Défense Nationale

Published since 1939 by the Committee for National Defence Studies, *Revue Défense Nationale* has since then concerned itself with looking at new ideas on the big national and international issues from the viewpoint of security and defence. Its editorial independence allows it to participate actively in revival of the strategic debate in France and in promoting it in Europe and the rest of the world. www.defnat.com See

P.-S.

Charles Bwele is a consultant on information technologies, multimedia designer, co-founder and member of *Alliance géostratégique* (www.alliancegeostrategique.org) and writes the blog Électrosphère (http://electrosphere.blogspot.com)

Notes

[1] In computer security terms, a logic bomb is the part of a virus, a Trojan Horse or other malware which contains functions intended to cause damage to the infected computer. A logic bomb is therefore the payload of the malware (see Wikipedia).

[2] This term denotes a range of interconnected software robots installed on a large number of machines. Any computer connected to the Internet can be infected by a botnet and then controlled by a hacker without the knowledge of the user.

[3] A rootkit is software whose purpose is to obtain and keep unauthorized access in the stealthiest way possible to the resources of one or more machines (time processor, network connections, etc.). In this way, these machines become the targets or vectors of a cyberespionage operation or an online attack.

[4] In IT terms, pervasive describes something which spreads to all parts of an information system.