The War of Attrition in Cyber-Space or "Cyber-Attacks", "Cyber-War" and "Cyber-Terrorism"

Eduardo Gelbstein

Has over 40 years experience in information systems and technology, both in the private and public sectors. His experience includes being Information Technology Strategy Manager for the British Railways and Director of the United Nations International Computing Centre. He was also an advisor to the United Nations Board of Auditors and the French Cour des Comptes. Ed is currently Adjunct Professor at Webster University Geneva and the author of several books and articles as well as a regular speaker at international conference on security, risk, audit and governance.

Resumo

A Guerra de Atrição no Ciberespaço ou "Ciberataques", "Ciberguerra" e "Ciberterrorismo"

Nos últimos anos tornou-se óbvio que o mundo virtual das bases de dados e do *software* – popularmente denominado como ciberespaço – tem um lado negro. Este lado negro tem várias dimensões, nomeadamente perda de produtividade, crime financeiro, furto de propriedade intelectual, de identidade, *bullying* e outros.

Empresas, governos e outras entidades são cada vez mais alvo de ataques de terceiros com o fim de penetrarem as suas redes de dados e sistemas de informação. Estes vão desde os adolescentes a grupos organizados e extremamente competentes, sendo existem indicações de que alguns Estados têm vindo a desenvolver "*cyber armies*" com capacidades defensivas e ofensivas.

Legisladores, políticos e diplomatas têm procurado estabelecer conceitos e definições, mas apesar da assinatura da Convenção do Conselho da Europa sobre Cibercrime em 2001 por vários Estados, não existiram novos desenvolvimentos desde então.

Este artigo explora as várias dimensões deste domínio e enfatiza os desafios que se colocam a todos aqueles que são responsáveis pela proteção diária da informação das respetivas organizações contra ataques de origem e objetivos muitas vezes desconhecidos.

Abstract

Over the last few years it has become obvious that the virtual world of data and software – commonly referred to as cyberspace, has a dark side. This dark side has many sides, notably loss of worker productivity, financial crime, theft of intellectual property, identity theft, bullying, and more.

Companies, governments and others are increasingly being targeted by largely unknown parties attempting, often successfully, to penetrate their networks and disrupt their information systems and data. These parties range from the individual teenage hacker to highly competent groups, and it is alleged that a growing number of countries are developing "cyber armies" with defensive and offensive capabilities.

Legislators, politicians and diplomats struggle with concepts and definitions (e.g. can malicious software be treated as a weapon?) and, apart from the Council of Europe Convention on Cybercrime issued in 2001, which has been adopted by a small number of countries there are no other treaties.

This article explores the many dimensions of this domain and highlights the challenges faced by practitioners charged with protecting their organization's information assets from unknown attackers with unknown objectives.

This paper explores some of the consequences of the convergence of the physical world and the virtual world of information, data and the (physical) systems used to process and disseminate them, now referred to as "cyberspace".

The assumptions on which this paper is based are:

- Assumption 1: computer systems and networks are ubiquitous. Their technologies, software and the operational processes needed for them to function all have intrinsic vulnerabilities. This makes them "insecure by design".
- Assumption 2: societies have become irreversibly dependent on them to the extent that they are critical to their functioning. Examples include utilities (electricity, water, and telecommunications), transport (ports, railways, airports and air traffic control), finance (funds transfers, banking and insurance), law enforcement and the military, logistics and supply chains and many more. This makes them attractive targets to any party wishing to disrupt a society.
- Assumption 3: conflicts (war, terrorism and other) have so far taken place on land, water and air. Much has been written about the potential of their extension to space given that satellites are used for telecommunications and intelligence gathering by both, civilian and military organisations. It is plausible to assume that cyber-space will also, sooner or later, be used in conflicts at least as a complement to more conventional actions.
- Assumption 4: attacks on the availability, confidentiality and integrity of data have been taking place well before computers were adopted. The hyper-connected world of today and the growing number of individuals with access to cyberspace makes easier for such attacks to be organised and launched, often successfully.
- Assumption 5: legislation applicable to Cyberspace is evolving. Its development is slow compared to that of innovation, both technical and of services, the latter ranging from electronic commerce and its related financial services to social networks and much more. One of the obstacles to the development of legislation is lack of agreed terminology and definitions.
- Assumption 6: the lack of a consistent national framework for cyberspace legislation is, in turn, an obstacle to the development of international treaties. Their absence inhibits international cooperation in identifying the sources of attacks if cross-border data traffic is involved as well the investigation and prosecution of suspected actors.

The sections that follow explore many of these topics in more detail.

Tower of Babel: from Definitions to Legislation

Terminology

New terminology is created continuously. It is appropriate to recall the story of the Tower of Babel[1] "let's… confuse their language so they will not understand each other" which remains valid today as innovations add words to our vocabularies. For example:

The word "cyberspace" first appeared in William Gibson's 1984 book "*Neuromancer*". It was used to describe the electronic medium of computer networks in which communications take place in real time. Other definitions exist, of course, and they have both supporters and critics.

Expressions such as "cyber-terrorism" and "cyber-war, (and variants of them) have been in use for many years. The media uses such terms liberally with little regard for detailed definitions. Academics, researchers and authors have put forward several definitions that remain a topic of debate.

The literature credits the first use of the expression "cyber-terrorism" to a 1996 article by Barry Colin, a senior researcher at the Institute for Security and Intelligence in California that states:

> *"The physical and virtual worlds are inherently disparate worlds. It is now the intersection, the convergence, of these two worlds that forms the vehicle of Cyber Terrorism, the new weapon that we face."* (Colin, 1996).

Another definition given by Major Bill Nelson of the U.S. Air Force states:

> *"Cyber-terrorism is the calculated use of unlawful violence against digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological."* (Nelson *et al*., 1999).

The fact remains that the phrase *"One man's terrorist is another man's freedom fighter"* (Seymour, 1975) is as valid today as it was when it was first used. Besides, some individuals referred to at one time as "terrorists" have since become democratically elected politicians in government. A few of them became Nobel Peace Prize Laureates. Clearly, labels can be misleading and are not permanent.

When it comes to "cyber war" (or warfare) the same applies – the term is widely used but definitions remain debatable. One example can be found in a 2004 report that puts emphasis on nation-state boundaries:

[1] Verse 11:7, Genesis, The Bible.

> *"Cyber warfare involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means."* (Billo *et al*., 2004).

In his 2010 book "Cyber War", Richard A. Clarke defines Cyber-Warfare as:

> *"Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."*

Lawyers are more cautious as terminology is fundamental to legislation and legislation is a pre-requisite for prosecution. This is illustrated by the well-known opinion (on a different subject) given by a Judge in 1964:

> *"I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description "hard-core pornography"; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it, and the motion picture involved in this case is not that".*[2]

Diplomats, politicians and military personnel as well as international organizations, continue to debate how to formalise definitions of "cyber-war" and "cyber-terrorism" as well as philosophical issues such as whether software can be used as a weapon. It would not be reasonable to expect quick answers.

Legislation for Cyberspace Crime and Conflict

Computer Misuse and Crime

The scope for computer misuse is huge and limited only by the creativity of the parties engaging in this. While many countries have been working for years to introduce appropriate (national) legislation[3] to address this, loopholes remain in such legislation. This in turn presents challenges in bringing criminals to justice.

The main problem is the lack of international harmonization of cybercrime legislation. Investigation and prosecution are virtually impossible if some activities in cyberspace are considered to be a crime in one country but not in another.

The only international instrument on cyberspace related topics known to the author is the Council of Europe Convention on Cybercrime, agreed in 2001 and which entered into force in 2004. By 28 October 2010, 30 countries had signed and ratified the convention. An additional 16 countries have signed the convention but

[2] Justice Potter Stewart, opinion on *Jacobelli vs. Ohio*,1964.

[3] *E.g.* in the U.K. the Data Protection Act (1988) and the Computer Misuse Act (1990) (and more…).

not ratified it. It should be remembered that the United Nations had 193 Member States (in May 2012).

As an illustration of the complexities of cross-border activities in cyberspace, is the case of Gary McKinnon, a UK citizen accused by the United States (both countries are signatories of the Council of Europe Convention) of hacking into 97 databases of the US Military and of the space agency NASA over a period of 13 months in 2001-2. These activities included deleting critical files and posting a notice "your security is crap".

Extradition proceedings against McKinnon were started by the United States in 2005 and the legal process continues through a sequence of appeals.

An initiative being progressed by the International Telecommunications Union (a United Nations specialised agency) to support nations in the harmonisation of policies (leading to legislation) can be found in the public domain.[4]

Laws of Conflict

The Laws of War *(Jus in Bello)* have a long history, which is likely to precede the invention of writing. These laws attempt to regulate the conduct of Nations, armies and individuals in a conflict statements to this effect can be found in the Hebrew Bible (book of Deuteronomy) and in the Koran (*Sura-al-Baqara*).

Today there are many international treaties on the laws of war (or Laws of Armed Conflict,[5] LOAC) – the First Geneva Convention entered into force in 1864 and the latest treaty found, the Convention on Cluster Munitions, entered into force in 2010.

Each one of the laws or conventions was developed after some new weapon or technology has been used in conflict. When it is felt that its consequences are unacceptable, politicians and diplomats seek some kind of mutual agreement to avoid or limit their use. This process can take many years and has not stopped various parties in conflict from ignoring such laws or conventions.

From time to time, the international community refers such situations to an independent body such as an international (war crimes) tribunal or the International Criminal Court. Once again, these processes are lengthy and are supported by existing legislation.

None of the treaties in force covers the use of information and/or software as disruption tools or as weapons. Similarly, attacks on computer systems and data are not mentioned in any of the current Laws of Armed Combat, the Geneva Conventions or any other treaties.

In past years past there have been United Nations (2004) documents on cyber-security and also Resolutions relating to cyber-security (none appears to be dated

[4] Available at http://www.itu.int/ITU-D/projects/ITU_EC_ACP/index.html.

[5] Available at http://usmilitary.about.com/cs/wars/a/loac.htm.

later than 2009). Similarly, the International Telecommunications Union has implemented a Cyber Security Agenda and also passed a number of related Resolutions. In their present form, these do not constitute a legal framework or a treaty.

Other international organisations, notably the Organisation for Economic Cooperation and Development (OECD) have done research and issued publications. In a recent report the author's state: *"it is extremely unlikely that there will ever be a true cyberwar"* (OECD, 2011).

The caveat is that the authors define "cyberwar" as one that is fought exclusively in cyberspace. They do acknowledge that cyber-weapons are already in extensive use and that a conventional conflict that includes cyber attacks is a distinct possibility.

A comprehensive multidisciplinary report on these issues was presented to the French Senate on 18 July 2012 (Bockel, 2012). It includes a detailed discussion of the defensive and offensive cyber-strategies of several countries.

There are more initiatives and publications by other organisations. Some are International Organisations, such as the Organisation for Security Coordination in Europe (OSCE) while others are non-governmental organisations, as is the case with ICT4Peace Foundation.[6] The latter published a report on the promotion of peace in cyber-space (Stauffacher, Sibilia and Weekes, 2011).

It can be assumed that most countries are developing defensive capabilities as it has become evident that attackers of many kinds have acquired strong capabilities to launch Advanced Persistent Threats. In parallel, there are also many reports of Nations developing cyber-attack capabilities – some list a handful of countries known or suspected to have such capabilities. Other reports[7] such as the one by the security company *McAfee* in 2007 stated that up to 120 countries were then engaged in cyber espionage and other forms of attack.

The issue remains that by mid-2012 there appears to be a fair consensus that the existing Laws of Armed Combat and the various treaties (such as those of the United Nations and the North Atlantic Treaty Organization (NATO) may not adequately cover all the issues relating to cyber-warfare and/or terrorism.

What the international community should have learned from developing treaties is that they take an inordinate time to be developed and that when completed, some nations will not sign or ratify them.

Just to provide a couple of examples, this has been the case with:

- The United Nations Convention on the Law of the Seas (UNCLOS), developed between 1973 and 1982, has been signed by 162 countries. Amongst the non-signatories is the United States of America – in July 2012, the Senate

[6] Available at http://www.ict4peace.org.

[7] *"Government-sponsored cyberattacks on the rise"*, available at http://www.networkworld.com/news/2007/112907-government-cyberattacks.html.

could not muster the necessary majority to ratify the treaty on concerns that doing so would constitute an erosion of U.S. sovereignty, both in terms of international arbitration of disputes and the possibility that a supranational body could impose binding rulings on the U.S.

- The Treaty on the Non-Proliferation of Nuclear Weapons (NPT) ratified in 1970 and signed by 190 countries. Four countries are not parties to this treaty. Of them three, India, Pakistan and North Korea have openly tested such weapons. A fourth country - Israel - is believed to have such weapons but has never declared such ownership. North Korea announced its withdrawal in 2003.

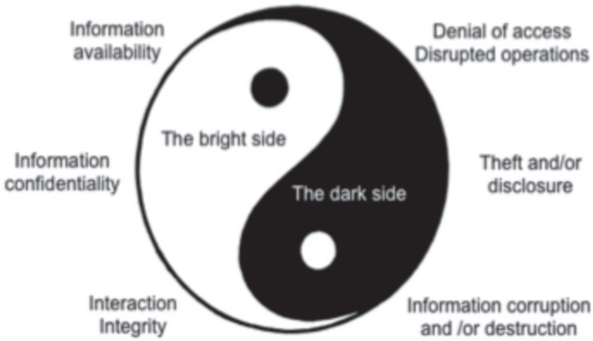
Non-state actors ignore such treaties and conventions.

The current status of the laws of conflict did not inhibit statements on the subject made public such as the two examples that follow: in May 2009, General K. Chilton, U.S. Military Strategic Command said[8] that: "In the event of a cyber-attack, the Laws of Armed Conflict will apply."; in October 2011, General R. Kehler, from the same organization said[9] that: "… there is a need to define Rules of Engagement for Offensive Computer Warfare." Readers are invited to draw their own conclusions.

The *Yin* and the *Yang* of Cyber-space

Chinese philosophy gave us the concept of *Yin-Yang* (translated as "shady place" and "bright" or "sunny" place). These are complementary, not opposing, forces that interact as part of a dynamic system. Everything has *Yin* and *Yang* sides and the boundary between them can change with time.

In cyberspace these sides can be seen as:


Information availability
Denial of access Disrupted operations
The bright side
Information confidentiality
Theft and/or disclosure
The dark side
Interaction Integrity
Information corruption and /or destruction

[8] "Official: No options 'off the table' for U.S. response to cyber attacks". Stars and Stripes, 8 May 2009.

[9] "U.S. Weighs Its Strategy on Warfare in Cyberspace". *The New York Times*, 18 October 2011.

On the *Yang* or bright side, cyberspace has provided the world with:

- Unprecedented possibilities for the creation and sharing of data and information;
- Standards to enhance connectivity and data exchanges in critical infrastructures;
- Social and professional networks for its dissemination and sharing;
- Online learning capabilities to reach anyone who wishes to learn;
- E-business and E-government;
- Useful tools for national defence and law enforcement;
- And so much more – creativity continues to drive the Yang (e.g. Apps for smart phones and new gadgets).

The consequence of this is that cyberspace is data and information-rich and these are valuable resources:

- Some data and information is public (anyone can access it but not necessarily make sense of it or vouch for its quality). Other data and information is restricted (access requires registration, sometimes a paywall);
- Much data is operational – not accessible to the public and rarely accessible to individuals (except for diagnostic purposes) – and part of what is called Systems Control and Data Acquisition (SCADA). This is a vital component of process management including for example electricity generation, air traffic control, telephone exchanges and virtually all of the infrastructures on which society depends;
- There is confidential data – accessible only to those meeting specific criteria (intellectual property, financial and legal data, medical records);
- Finally there is secret data – not shared other than within a very small circle of qualified and nominated people (passwords, national security and law enforcement).

However data and information that have value are of interest to many groups: spies (industrial and other), criminals (fraud, theft, extortion), law enforcement (intelligence acquisition and analysis, tracking, planning) and many others.

Such data can be acquired legitimately either because it is in the public domain or the individual has the appropriate permissions to do it.

The *Yin* side has also many elements to consider:

- Irreversible dependency on cyberspace for many, if not most, critical activities;
- Questionable Quality Assurance for much of the information and knowledge disseminated;
- The dissemination of Non-Knowledge: misinformation, disinformation, proselytization, etc.;
- Cyber-crime – non violent and profitable;
- Theft of intellectual property and other forms of espionage;

- Hacktivism – attacks on cyberspace residents for any of a variety of reasons;
- Cyber-attacks on information infrastructures by non-state actors (could also be state sponsored);
- Cyber-attacks on information infrastructures by hostile nation states.

Those in the *Yin* side of cyberspace ("uncivil society" as former U.N. Secretary General Kofi Annan called them) can access data without permission by breaking into systems. This may be relatively easy to do if the protective measures taken are. However, events that took place in recent years indicate that any system can be broken into if the attackers have the skills and resources to implement an Advanced Persistent Threat. This may be illegal depending on the legal framework of the location where such break-in takes place. A relatively small number of offenders has been apprehended, judged and sentenced.

Once they break into a system, intruders may do many (all bad) things:

- Disruption – website defacement, denial of service, encrypting data and denying access to it by its rightful owners,
- Strategic advantage through espionage – advanced information on mergers and acquisitions, exchanges of sensitive information, intelligence gathering, etc.
- Financial gain – phishing, stealing intellectual property, fraud in various forms;
- Sabotage (including terrorist acts) – interfering with the operation of critical processes;
- Military uses that exploit the gaps in the Laws of Armed Combat and current treaties; and more…

Technologies in Crime and Conflict

Fighting has existed for as long as the human race. It has been given many names, including "conflict", "terrorism" and "war". Some fighting has been formalised and codified, by for example the Laws of Armed Combat and the Geneva Conventions. However, much fighting is not subject to any such rules.

History shows that the tools for fighting have evolved as technical innovation progressed – from slings and stones to bows and arrows, fire, axes and maces, swords, gunpowder leading to rifles, pistols and cannons and so on (Alvin and Heidi Toffler, 1993).

The industrial revolution (1750 to 1850) resulted in changes in technology, manufacturing, transport as well as in society. It was also the start of the formalisation of management. All of these were adopted by the military and law enforcement (it could be argued that the legions of the Roman Empire already applied "management").

Technologies such as motorized vehicles and aircraft extended the reach and speed with which fighting could be carried out. Developments in electronics around the time of the Second World War brought innovations such as radar and sonar, devices to facilitate (and break) encryption.

New forms of weapons, notably the atomic bomb were also turned from theory to reality leading to the doctrine of Mutually Assured Destruction.

Since then, rapid innovation in Information Technology has enabled new facilities. These include sophisticated information analysis and its dissemination in the field, satellites for information gathering and communications, "smarter" weapons including precision guided missiles, drone aircraft, robots and more.

Some of these technologies have become commodities. One of them, the smart phone, which includes photographic and video capabilities, access to GPS data and access to the Internet, are also being used by opponents engaged in asymmetric conflict (variously referred to by the media and others as "terrorists", "hacktivists" or "hackers" – all of these may be correct to somebody, somewhere, sometime).

The concept of Information Warfare (IW) originated in the United States of America and uses information technology to gain advantage over an opponent by collecting tactical information, enabling "dis" and misinformation to be disseminated, denying information collection to the opponent and protecting one's own systems and data (Denning, 1998). Other countries refer to such activities as Information Operations. Courses on Information Warfare are offered by many military academies around the world.

It is almost certain, that many Nation States use electronic means to gather intelligence. It is also a fact that every organization that uses computer systems and networks takes steps to provide defences for their protection. The global media speculates that a number of Nation States are developing offensive cyber-capabilities and uses terms such as "cyber-armies".

A conflict in which computer systems and networks are considered legitimate targets would have massive impact: all the infrastructures critical to the functioning of society – utilities, telecommunications, transportation, banking and finance, supply chains, etc. rely extensively on information technologies and networks and are therefore highly vulnerable to attack by hostile parties.

The concept of "Economic Jihad" (The Economist, 2008) – attacks that damage the economic interests of a nation or its enterprises and financial institutions – has been voiced many times over the last few years. Given that so many critical activities now make use of cyberspace, such attacks should be considered a real threat.

The remainder of this article explores the many dimensions of these challenges.

Selected Cyber-events that Actually Occurred

Fiction has already explored forms of attack for years and some of them have actually happened while others are perhaps just waiting for the opportunity.

Here is a short selection of events yet to happen:

- Arthur Clarke's "2001" (1968) in which an artificial intelligence computer called HAL kills an astronaut to keep secret the mission for which it was programmed.
- Henning Mankel's "Firewall" (1998) in which a persuasive and talented IT specialist plans to create worldwide financial panic by deleting large amounts of money from the banking system. This is not likely to have been the reason for the financial crises that began in 2007…
- Michael Dobbs "Edge of Madness" (2008) in which a Chinese dictator declares cyber-war against the West and includes airplanes falling from the sky, power failures, transport breakdowns and a runaway nuclear power station.

However, the following did happen:

- On 14 August 2003, a massive blackout impacted 65 million people in Canada and the Eastern United States. Officials issued statements that "terrorist activity was not the cause" and identified a combination of factors, including computer errors.
- On 28 August 2003, a blackout affected southern London and Northwest Kent. The official explanation involved two independent faults happening within 7 seconds from each other.
- On 23 September, another blackout affected the southern part of Sweden and the eastern part of Denmark, affecting 4 million people. This was reported to be the consequence of the abrupt stoppage of a Swedish nuclear power station.
- On 28 September 2003 a massive blackout covered the whole of Italy (except for the islands of Sardinia and Capri) and impacted 56 million people. A part of Switzerland was also affected for several hours. The official explanation involved storm damage.

Officials have dismissed the idea that these blackouts were the result of "proof of concept attacks". However, the probability that these closely spaced events were random should be regarded as small as blackouts happen around the world regularly and their main primary cause is the weather.

The above events do illustrate the impact of deliberate action on computer systems could have. The difference would be that a well designed attack involving sophisticated malware would be difficult to diagnose and repair.

Between 23 January and 4 February 2008 there were disruptions due to separate incidents due to damage to Internet underwater cables. The first incident caused damage involving up to five high-speed Internet submarine communications cables in the Mediterranean Sea and Middle East from, causing disruptions and in the Middle East and India.

The U.S. government reported a series of coordinated attacks on computer systems since 2003 (such attacks continue today) and gave the collective name of "Titan Rain". While their exact source remains unknown the attacks are suspected to be state sponsored and intended to gather information. The Titan Rain hackers gained access to many computer networks, including those of defence contractors such as Lockheed Martin, and NASA.

A series of distributed denial of service (cyber) attacks on Estonia began on 27 April 2007 and swamped websites of Estonian organizations, including the parliament, banks, ministries, newspapers and broadcasters. These attacks followed the relocation of the Bronze Soldier of Tallinn as well as war graves in Tallinn. Other attacks involved high volumes of spam on news portals commentaries and the defacement of selected websites.

It was thought at the time that these attacks were of a sophistication not seen before. These attacks have become a case study for many military planners as, at the time it took place, it may have been the largest instance of a cyber attack believed to be state-sponsored. No country has claimed responsibility for these attacks.

On 5 August 2008, three days before Georgia launched its invasion of South Ossetia, the websites for OSInform News Agency was hacked. Website kept its header and logo, but its content was replaced. Alania TV, a Georgian government supported television station denied any involvement in the hacking of the websites.

A related cyber attack on the websites of the Parliament of Georgia and the Georgian Ministry of Foreign Affairs replaced images of the Georgian president. Other attacks involved denials of service to numerous Georgian and Azerbaijani websites. The governments of Estonia, Ukraine, and Poland offered technical assistance and mirrored web pages for Georgian websites to use during the attacks

In June 2010 malware named *Stuxnet* was discovered and identified. It was found to have been specifically designed to attack supervisory controls and data acquisition (SCADA) systems designed by Siemens and used to target the uranium enrichment centrifuges at the Natanz plant in Iran. Other countries have been reported to have been also infected.

Press reports suggested that it made the control systems operate so as damage the centrifuges while displaying normal operations to the controllers. The authorship of *Stuxnet* remains speculative. It has been suggested that the development of such sophisticated malware would require government resources.

Stuxnet (and subsequently deployed malware, notably *Duqu* and *Flame*) can be considered to be the first weapons-grade malware. An analysis of *Flame*, first discovered in May 2012 is reported as being the most sophisticated found so far and it was used to gather intelligence by recording screenshots, keyboard actions and audio (including Skype conversations).

While the theft of intellectual property and other forms of intelligence gathering (espionage) have not been mentioned in this section as they are common enough event, the Director General of MI5 (the UK's internal security organisation) said in a speech in London on 25 June 2012, that one area of increasing concern is the threat posed by state-sponsored cyber espionage. He also said that his organization would only get involved in such cases if such thefts or disruptions posed a potential threat to national security.[10]

Insider Threats

The information security industry places much emphasis on the actions of external parties, generally described as "hackers". In reality, the insider threat must not be ignored.

Misusing computer systems to bypass controls can have significant impact, something that three major banks experienced directly. While the three cases below received considerable media attention, such events are likely to occur "everywhere". It was just the magnitude of the impact that made them known to the world:

In 1995, a trader at the Singapore branch of Barings Bank (the oldest merchant bank in London), Nick Leeson, lost £837 million in speculative in future contracts. The bank collapsed.

In January 2008, a French trader, Jérôme Kerviel was convicted of causing the French bank Société Générale a trading loss valued at €4.9 billion through forgery and unauthorized use of the bank's computers. The case was being considered by the Court of Appeal at the time of writing.

In September 2011, the Swiss bank UBS reported the loss at their London offices of over $2 billion, as a result of unauthorized trading performed by Kweku Adoboli. This event has not yet gone to trial.

Other insiders may exploit access rights for an unintended purpose:

Bradley Manning, a U.S. soldier, was arrested in Iraq in May 2010 on allegations of having given classified material to the WikiLeaks organisation. He was subsequently charged with several offences, in particular that of communicating national defence information to an unauthorized source

Just before WikiLeaks was due to post the documents (mostly diplomatic cables) received from Manning, it was the target of a massive Denial of Service attack. A person using the pseudonym "Jester" claimed to have organised the attack on the grounds that such disclosure "threatened the lives of our troups."

This was followed by the removal of the Wikileaks website and data by service providers. Shortly after Paypal, an online payments company cut off the accounts used by WikiLeaks to collect donations and two credit card companies, Visa and Mastercard stopped payments to WikiLeaks. The Swiss postal bank, Postfinance,

[10] Available at http://www.guardian.co.uk/uk/2012/jun/25/mi5-uk-terrorism-threat-warning.

froze the assets of Julian Assange, founder and editor-in-chief of WikiLeaks.
Anonymous' reaction: Responding to perceived federal and corporate censorship of the cable leaks, internet group Anonymous attacked the websites of, among other PostFinance, MasterCard and Visa with Distributed Denial of Service attacks.
John Perry Barlow, co-founder of the Electronic Frontier Foundation, wrote[11] about these events saying that: "The first serious infowar is now engaged. The field of battle is WikiLeaks. You are the troops."

Open Issues and Questions Looking for Answers

A substantial number of governments are fully aware that cyber attacks are happening and are against their national interest. The website of NATO's Cooperative Cyber Defence Centre of Excellence, located in Tallinn, Estonia, includes a page[12] with links to documents on national cyber / information security.

The same organization also runs courses on public international law as it applies to cyber operations, including, inter alia, issues such as the prohibition of the use of force, the law of self-defense, countermeasures, LOAC, the law of neutrality, legal attribution and State responsibility. The course as run in 2012 is classified NATO SECRET and participation requires the appropriate clearance.

The open issues are many and relate to questions to which currently there are no accepted answers.

Open Issue 1: Identifying the Attacker

So far, attackers have not identified themselves other than by citing membership of a group (such as Lulszec or Anonymous) whose members are dispersed around the world and without a formal structure. Any statement pointing to a Nation's cyber-army is essentially conjectured.

The complex architecture of the Internet and the fact that it was never designed to be a secure network allows attackers to be anonymous and to hide in the network maze. This gives them plausible deniability and, at the same time, creates barriers to investigators that are complex, time consuming and, potentially, not possible to overcome.

As a result, investigating, collecting evidence that would be accepted in a court of law and prosecuting cyber criminals is immensely for law enforcement. This is aggravated by the inability to recruit and retain expert staff. A recent campaign by the UK's Government Communications Headquarters[13] (GCHQ) in which people were invited to decrypt a message placed on a website revealed that the salary on

[11] Available at http://twitter.com/jpbarlow/status/10627544017534976.

[12] Available at http://www.ccdcoe.org/328.html.

[13] Available at http://www.gchq.gov.uk/challenges/pages/break-some-code-puzzle-1.aspx.

offer was less than half of what a person with such skills could earn in the private sector.

Open Issue 2: Legal Framework Relating to Cyber-attacks

The development of a good legal framework remains a challenge given that legislation develops much more slowly than technical innovation and the creativity of attackers – whoever and wherever they may be. National initiatives are progressed following different strategies and priorities and with little or no international collaboration, despite the existence of appropriate forums for this to take place (such as the U.N. and its Agencies, Interpol, Europol, OECD, OSCE, ENISA, WSIS (World Summit for the Information Society), etc.).

Open Issue 3: Can Software be a Weapon?

Given that software is an intangible element the intuitive response could be "I don't see how". As it happens, a recent issue of the journal "*The Economist*" explores this from a different perspective: the extent to which electronics are used in health care – from robots performing surgery to defibrillators, pacemakers and insulin pumps – all of which are susceptible to software errors and/or attack, so, yes, software could kill you directly.[14] As is the case with most software, the end user license absolves the supplier and/or designer from all liabilities.

The consequences of an attack on what would normally be a protected infrastructure, such as a hospital, could also be bad for peoples' health. The same is true for interference with water supplies, air traffic control and so many more.

The *Stuxnet* malware also demonstrated that software could be used to damage a physical object while being much cheaper to develop and easier to deliver.

The author could not find any reference to software being classed as a weapon in any legislation in English.

Open Issue 4: How do you Inspect Software Looking for Malware?

The United Nations has over the years had many weapons inspection missions. While no doubt complex and sensitive, such inspections focused on tangible items that could be counted, measured, weighed and generally evaluated.

As software is none of those things and its documentation may not be available to eventual inspectors, the task becomes much more complex. The people with the skills to identify malware (after it's been used) and analyse it and published reports are primarily working for companies supplying anti-malware tools, including Kasperski, McAfee and Symantec (listed alphabetically).

[14] *"When code can kill or cure". The Economist*, June 2, 2012.

Open Issue 5: the Case for a Convention on Cyber-weapons and Related Matters

Numerous parties have suggested that such a convention would be a timely addition to the current portfolio. Should it be developed and, if so, who should do it and how can compliance be assured? At the time of writing there did not appear to be any such initiative.

Following from open issues 1 to 4, some of the questions looking for answers would include:

Is there an appropriate model for such a convention, and if so, which one: possible models include the Council of Europe Convention on Cybercrime and the United Nations Convention on the Law of the Sea (UNCLOS) already mentioned in these pages.

Such a convention could also extend the scope of the current Laws of Armed Combat and relevant Geneva conventions to cover items such as:

- Would an unannounced or undeclared attack seen as a pre-emptive strike constitute an act of war?
- How does the concept of lawful targets and protected targets apply to computer systems and networks?
- How should "proportionality" be assessed in a response to an attack?

Which would be criteria defining when to involve law enforcement and the military?

- Who would have the authority to take such decisions?
- Can and should governments intervene if an attack targets an organization in the private sector (for example, a utility)
- Under what circumstances can the government if targeted by a cyber attack seek the collaboration of the private sector?

The two issues that are likely to remain open indefinitely are those of Nations that do not sign the convention and non-state actors that ignore the convention altogether.

Conclusions

Technical innovations have invariably found their way into law enforcement and defense establishments on land, sea, air and space. Now they also appear in the world of computer systems, networks and data called "cyberspace".

They have also been used for criminal activities and in conflicts and there is no reason to believe that this will change any time soon.

The factors that distinguish conflict in cyberspace include:

- Malicious software (malware) can be designed anywhere and by anybody who has adequate expertise and skills. These skills are not particularly difficult to acquire and toolkits to manufacture malware can be procured easily and cheaply enough around the world. Not all malware is detectable;

- Malware designers are good at sharing knowledge, software programs and tools. They have associations, clubs and conferences. Some of the latter, such as Defcon, are annual public events;
- Attacks on computer systems are mostly asymmetric: a small number of players can successfully penetrate and interfere with the computer systems and the defences of large organizations in the private and public sectors, including defence establishments.
- The sophistication of attacks in cyberspace continues to grow. It is now legitimate to think in terms of Weapons-grade Malware. Attribution is a major obstacle as the attackers' anonymity is hard to unravel. Without certainty, the only practical response should focus on defensive actions and recovery.
- The insider threat must not be underestimated: insiders have knowledge and opportunity. They may be driven to act by ideology, external pressures and emotion. The spectrum of such drivers is large and includes lack of awareness and stupidity.
- External attackers are exposed to little risk – a failed attack still provides useful information of what did or did not work and insights into the defences of the target. Besides, attackers can hide their identity and location without too much difficulty and remain anonymous. Even if caught, arrested and extradited, the legislative framework varies from country to country and requires a long process. Such a process could encourage other attackers to focus on those driving it.
- The concept of Mutually Assured Disruption has not been the subject of much public discussion are remains a source of potential social unrest as interference with water and electricity supplies, banking services, transportation, etc. are bound to cause friction if they last long enough.

Many countries have created bodies to coordinate the protection of critical national infrastructures and their activities should continue to be encouraged, supported and shared. The actual response capabilities of such infrastructures to respond to a cyber-attack remain to be seen.

References

Billo, Charles *et al*. (2004). *Cyber Warfare: an Analysis of the Means and Motivations of Selected Nation States.* Darthmouth College: Institute of Security Technology Studies.

Bockel, J. M. (2012). *Rapport d'information No. 681*. Available at http://www.senat.fr/rap/r11-681/r11-6811.pdf.

Clarke, Richard (2010). *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Harper Collins.

Collin, Barry (1996). “The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge”. Available at http://thecampuscenter.com/cgi-bin/texis/.

Denning, Dorothy (1998). *Information Warfare and Security*. New York: Addison-Wesley.

Nelson, Bill *et al*. (1999). *Cyberterror, Prospects and Implications.* Center for the Study of Terrorism and Irregular Warfare.

OECD (2011). *Reducing Systemic Cybersecurity Risk.*

Seymour, Gerald (1975). *Harry's Game.* New York: Random House.

Stauffacher, D.; R. Sibilia and B. Weekes (2011). *Getting Down to Business – Realistic Goals for the Promotion of Peace in Cyber-space.* ICT4 Peace Foundation.

Toffler, Alvin and Heidi Toffler (1993). *War and Antiwar.* New York: Little and Brown.

United Nations (2004). *A More Secure World* - *Report of the Secretary General's High Level Panel on Threats, Challenges and Change*. New York: United Nations.