CYBERWARFARE AND ITS DAMAGING EFFECTS ON CITIZENS

STEFANO MELE
Cyberwarfare
and its damaging effects on citizens

by Stefano Mele

[ September 2010 ]
Contents

1.0 Introduction ......................................................................................................................... 5
2.0 Virtual conflict, real damage ............................................................................................... 10
3.0 Data and statistical elements related to the threat............................................................... 15
4.0 Conclusions .......................................................................................................................... 17
Biographical notes....................................................................................................................... 19
1.0 Introduction

In order to analyze the real damage that a hypothetical cyber-war or individual act of cyberwarfare could do to the citizens of any nation coming under attack, it is fundamental to begin with some reflections which will help us reach a full understanding of the phenomenon, and its related practical implications.

The first of these is surely linked to the difficulty faced in defining the difference (which in the realm of cyber-space can be very subtle) between common criminals committing IT crime and so-called ‘cyber warriors’, by which I mean those individuals with a high level of technical skill who are paid by a State to commit acts of cyberwarfare. This is because, on a fundamental level, acts of cyberwarfare are often completely identical – technically speaking – to those acts which common criminals might commit over the internet: only the aims of these acts change (although sometimes even the targets are the same) along with those who conduct them, or order them to be carried out.

The classic quadri-partition of illegal acts within the realm of IT, as shown below, is therefore actually merely theoretical.
In addition, as is already known, it is not unusual for Governments to ‘dip a toe’ into the world of IT crime – organized or not – in order to carry out an individual cyberwarfare operation, or to reinforce their range of attacking options. This is especially true in cases in which the subject to be hired is capable not just of using those instruments or tools which can be found on the internet, but who is above all capable of creating such tools on an ad hoc basis for each specific act of penetration or manipulation of the target security system, and who is able to identify new bugs (the so-called ‘zero day’\(^1\) attacks) in the software used by Governments and individuals, so that defence systems do not already have the attack signatures of these bugs on their databases, thereby making such actions difficult to uncover.

Furthermore, we must consider that some types of illicit actions, although perhaps only those which are not considered by Governments to be too ‘delicate’, can be directly outsourced to specific private companies or criminal groups, which may also be foreign and without any geopolitical connections to events which could lead to cyber-war, and which would require, as an extra layer of security, the use of intermediaries both in initially obtaining the services of the company or the criminal group and in dealing with them, in such a way as to make more simple and immediate any public denial should an electronic attack come to be identified (a practice which is already common and widespread).

It follows on from these initial reflections, then, that beyond the commonly understood ease with which it is possible to remain completely anonymous in a conflict which, in its nature, is sometimes fought in a temporal arc of just tens of minutes, the problem of attributing responsibility for the attack does not just stem from the technical-structural elements of the web, and the material impossibility of putting a ‘face’ on its author, but also from the impossibility of pinpointing the precise geographical location of the attacker\(^2\).

It is also useful to point out, even as a brief mention, that in the overwhelming majority of cases of penetration and, even more so, manipulation of critical electronic national security systems, these

---

\(^1\) It must be noted, however, that in a recent study on the phenomenon of the so-called zeroday attacks and the relevance they actually have to the computer crime ecosystem, only a minimal and almost irrelevant percentage of attacks were carried out through the exploitation of errors of this kind, and that, instead, the majority of IT system violations are actually carried out via the exploitation of well-known bugs which have not been fixed with their relevant patches. For more information, see DAncho Danchev, “Seven myths about zero day vulnerabilities debunked”, at http://www.zdnet.com/blog/security/seven-myths-about-zero-day-vulnerabilities-debunked/7026?tag=mantle_skin%3Bcontent

\(^2\) General Michael Hayden, former director of the NSA, during a speech at the Black Hat conference, stated that a solution to the problem of attributing responsibility was currently being discussed and evaluated by the American Government, founded on avoiding searching for a precise ‘face’ (whether State or non-State) to be linked to one or more IT attacks carried out against America, but instead considering nations to be directly responsible for any damaging activities that originate in their ‘cyber-space’. 
are carried out (and will always be carried out) under the utmost secrecy\textsuperscript{3}. Even if it was possible to do so, the target State would only be able to find out if the attacking operation or the manipulation of electronic systems was successful or not if a real cyber-war was to break out, or only at the moment in which an act of cyberwarfare was carried out, and, therefore, those cyber-weapons which had been previously set up against an adversary would have to be used.

An additional mention in this analysis must be given to the consideration that the weakest link in electronic security systems has always been – and will be for a long time to come – man himself. And this is true both in terms of purely malicious, or intentional acts, and also in terms of unintentional failures.

In fact, as far any system can really be said to be ‘fully protected’ from external attack, it is certainly possible – if not highly likely – that disloyal employees may manipulate the network and its security systems from within, installing malware and/or modifying its security settings, thereby facilitating outside access. At its heart the history of espionage is full of traitors\textsuperscript{4} and double agents. It is not correct, therefore, to assume beforehand that such agents could not exist within the world of information security\textsuperscript{5}.

Different, but just as dangerous, is the purely random possibility that a lack of attention on the part of internal personnel, or an inadequate culture of security, or the fallacious assumption that a network, thought of as being inviolable from outside, can therefore be configured from within to be as useful and ‘elastic’ as possible, can lead to security systems being totally compromised. This, for example, occurred in 2008, when a file infected with malware originating from the non-secure network (NIPRNET) of the American Department of Defence was copied onto a USB pendrive, and was then uploaded onto a computer connected to the secure network (SIPRNET). The file was

\textsuperscript{3} The Wall Street Journal, however, in April 2009, revealed that Chinese and Russian spies have long been violating the electronic systems of United States National electricity grids, installing within them programs which can be activated over the internet, and which are capable of deactivating and/or destroying them within a matter of minutes. The article can be found here: http://online.wsj.com/article/SB123914805204099085.html

\textsuperscript{4} As an example of this, it is enough to remember that FBI agent Philip Hanssen, over 22 years of betrayal (from 1979 to 2001) and espionage carried out for the Russian Government, managed to photocopy and sell just a few hundred pages of classified documents, putting him himself directly at risk. Hanssen is currently serving out a life prison term, including 23 hours per day of solitary confinement.

Because of the internet and the digitalization of documents, however, the risk of being personally discovered during criminal acts has not only declined, but it is above all now possible to obtain many thousands of pages of confidential documents in an instant, and with extreme ease. Emblematic of this, recently, was the Wikileaks scandal over Afghanistan, which saw over 92,000 confidential documents made public, and the case of the young American intelligence analyst Bradley Manning, who is accused of making public, again via the Wikileaks portal, a video which documents military action carried out by the USA and of handing it over to a non-Governmental third party.

\textsuperscript{5} The events highlighted in the previous note have forced DARPA (the Defense Advanced Research Projects Agency) to develop, over the course of one month, a program known as CINDER (Cyber Inside Threat), through which it aims to try and stem the loss of confidential information from within the American defence sector by constantly monitoring the research, indexation and electronic copying of data.

Further information on this highly interesting project can be found at: https://www.fbo.gov/index?s=opportunity&mode=form&id=cf11e81b7b06330fd249804f4c247606&tab=core&tabmode=list&
opened, and the malicious software then spread uncontrollably, within hours infecting hundreds of terminals in Afghanistan, Iraq, Qatar, and, obviously, at American Central Command⁶.

A recent study from the DHS⁷, in fact, highlighted how the IT systems of US-CERT (United States Computer Emergency Readiness Team), which are used by the NCSD (National Cyber Security Division) in its mission to be the focal point in terms of cyber-security, both at the public and private level, suffer from numerous, and dangerous, vulnerabilities linked above all to the problem of a poor IT security culture amongst its employees. US-CERT, in fact, amongst other things, monitors the alert signals that ‘Einstein’, the intrusion detection system (IDS) which is tasked with monitoring the non-military networks of the US Government (the so-called ‘.gov’ systems), sends out in the event of any unauthorized attempted intrusions. This IDS system is also set up to send out, over the entire network it is in control of, notifications concerning software updates to be installed on the various computers which make up its ‘domain’, so that all users of the internal network are immediately warned of any eventual problems with security (bugs) found on the system, and so that patches for these bugs can be swiftly installed. This method, however, has been shown to be completely ineffective. Leaving the task of updating his or her machine to the end user, in fact, meant that, after a scan was carried out using the Nessus vulnerability scanner, 1,085 instances of 202 bugs pegged as ‘maximum risk’ - which could easily have been exploited for malicious purposes - were reported.

Finally, space must be left for a few brief reflections on the genuine probability of the break-out of cyber-war.

Even on the sole basis of the arguments analyzed thus far, it is logical to deduce that cyber-war is much more likely, and perhaps more convenient, than is currently predicted. A cyber-war, in fact, would even allow smaller States, which are normally incapable of competing either militarily or economically with larger international powers, to attack the critical systems of other State targets thanks to its excellent ‘cost-benefit’ ratio. In fact, by exploiting technical skills and know-how which in 90% of cases are available for no cost directly on the internet, and by exploiting the actually poor level of defence capabilities seen on this ‘battleground’ in all those nations (above all America) which are excessively dependent on technological systems, it is possible to bring this war to any part of the world, at low cost, and with a very high probability of obtaining a successful outcome.

It should also be highlighted that nations with a low level of IT development, for this very reason, retain at the same time a relative strength, and an insuperable defence strategy, with regards to

⁶ An event which was only recently acknowledged by US Defense vice president William Lynn III, following the publication in Foreign Affairs of an essay entitled “Defending a New Domain: The Pentagon’s Cyberstrategy”, available at http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain
any possible technological counter-attack which might be carried out by ‘highly digitalized’ nations, meaning they possess a kind of ‘general deterrent’ should acts of cyberwarfare be used, or should a real cyber-war break out.
2.0 Virtual conflict, real damage

What has been said thus far should lead to serious (and urgent) consideration being given not just to the general aspects of cyber-war and its related strategies of attack, defence and the mitigation of damage, but above all to the precise identification of what the primary targets within our national territory which can be attacked via the internet might be, even in the case of individual acts of cyberwarfare.

If we wish to refer only to targets where an attack could lead to the loss of human lives, we must highlight:

- electronic airport, civil and military air traffic and airspace control systems: although under current security procedures it does not seem possible that these could be used to cause mid-air collisions or other problems for aircraft coming in to land, it is however highly plausible that these airspace control systems could be remotely disabled, allowing, for example, carpet bombing of the territory by hostile aircraft without any early-warning alarms being set off.

---


9 The collision between two aircraft during landing is highly improbable, at least following an act of cyberwarfare by a foreign State, as cross-checks are carried out between the pilot of the aircraft and the control tower which, until it has the aircraft in sight, communicates with the pilot using radar data (position, speed etc.). The control tower ‘directs’ the aircraft from the moment its presence is detected in its airspace until it lands, giving it information on speed, when to change direction, and the height it must descend or ascend to, etc. Each command given to the pilot is immediately confirmed. This means that, even if some radar signals were to be falsified, which is certainly plausible, the pilot could always disregard those commands he receives in favour of what he himself sees from the cockpit during the landing phase, and his own instrumentation. Furthermore, a large number of sensors exist along runways which indicate the presence and position of other aircraft.

10 For a greater understanding of the American situation, an analysis of the U.S. DEPARTMENT OF TRANSPORTATION document entitled “Review of web applications security and intrusion detection in air traffic control systems” makes for interesting reading, available at http://www.oig.dot.gov/sites/dot/files/pdfdocs/ATC_Web_Report.pdf. This document sets out five security recommendations for the Federal Aviation Administration to apply to its air traffic control and management systems, with the aim of avoiding the possibility that these systems continue to be vulnerable to cyber-attacks. Actually, as can also be seen in this official document, (http://www.oig.dot.gov/sites/dot/files/Response%20Letter%20To%20Reps%20Mica%20Petri%20ATC%20Web%20Security%20Follow-up%2008-05-10.pdf), of the five recommendations, only four have currently been put into practice, with the recommendation relating to the adoption of intrusion detection systems remaining ‘open’ and incomplete.

11 This is what happened to the computers of the Syrian air defence systems when, in September 2007, they inexplicably did not signal the entrance into the National territory of Israeli Eagle and Falcon aircraft (which are not ‘stealth’ aircraft), which were capable of bombing a nuclear site.
- electronic control systems on civil and military aircraft: these systems becoming compromised can cause problems for aircraft during take-off and landing\textsuperscript{12}, in addition to, as was sadly demonstrated by Air France flight 447 in June 2009\textsuperscript{13}, aircraft falling out of the sky in mid-flight.

Despite this, at least as far as is known, not being the result of an actual malicious attack, this tragic event has demonstrated how current aeronautic (fly-by-wire) technology, in the event of any problems with the on-board computer, can irredeemably compromise the safety of the flight and of the passengers on that flight, giving the pilot very little chance to regain control of the aircraft.

- the electronic systems of companies which design and develop the hardware and software used in airports, in air traffic control and in the construction of aircraft, both civil and military: here, the objective is that of manipulating, in the design phase, software or hardware which will eventually come to be used in critical environments\textsuperscript{14}. The events linked to the theft of designs relating to the American F-35 project\textsuperscript{15} are an example of this kind of act.

It is also possible (although this would be difficult) that a hostile Government would not limit itself to simply copying confidential information, or carrying out acts of simple electronic espionage, but would aim to gain access to the plans, have them analyzed by its specialists, and introduce into the millions of lines of code which form the basis of the flight control software of an aircraft a small

\textsuperscript{12} Around the end of August, the Spanish newspaper \textit{El Pais} carried the news that the authorities investigating the Madrid air disaster of 2008 had discovered that one of the computer systems which monitored technical issues on the aircraft was found to be infected with malware. It is supposed, therefore, that one possible cause of this tragedy, in which 154 people died, was in fact the lack of an alarm warning of a technical malfunction, due to an infection within the control server. According to \textit{El Pais}, an internal compiled by the airline company revealed that that computer, which is situated at the Palma di Majorca headquarters of the airline, should have recognized at least three technical problems with the aircraft which, had they been correctly diagnosed by the server, would not have been allowed to take off. The Trojan virus, therefore, despite not having directly caused the incident, could have contributed to allowing an aircraft which should never have left the ground to do so. The final report on this event, however – which goes into greater detail – will only be made public in December. For now, for further details, see: http://www.elpais.com/articulo/espana/ordenador/Spanair/anotaba/fallos/aviones/tenia/virus/elpepiesp/20100820elpepinac_11/Tes

\textsuperscript{13} Detailed information on this event, above all focusing on what happened on board the aircraft before it crashed, can be found at: http://wikileaks.org/wiki/Category:Air_France

\textsuperscript{14} In fact, most electronic components currently used in all computers and mobile phones today are made in China, which is held, along with Russia, to be the most dangerous nation in the world in terms of the risks associated with cyberwarfare.

Not by chance, some months ago, India decided to ban, for security reasons, the use of electronic components sourced from China, in particular those produced by the two largest companies present in the territory, Huawei Technologies and ZTE. http://india.foreignpolicyblogs.com/2010/05/18/india-restricts-chinese-telecom-firms-citing-security-concerns/

\textsuperscript{15} For further details on this event, see “Computer Spies Breach Fighter-Jet Project” at: http://online.wsj.com/article/NA_WSJ_PUB:SB124027491029837401.html
‘backdoor’ – which would be hard to single out amongst the sea of information present – which would allow it to gain complete remote control of the aircraft. This manipulated code would then be reinserted into these previously violated systems. Once these are put into large-scale production, this ‘backdoor’ could then be used to make the aircraft fall out of the sky, or, in the case of military aircraft, to make it launch, for example, a missile with different target coordinates than had previously been set.

- electronic national defence systems, via which a ‘non-willed’ attack could be launched (even a simple long-range missile) towards the territory of a specific nation.

- fully-automated subway control systems: these do not require conductors or drivers to be present on trains, but feature, and are driven automatically, by ‘VAL’ systems. Compromising the security of these could lead to two trains colliding, or could cause individual trains to derail or travel beyond the end of the line, with a probable consequent loss of human lives.

- water supply and control systems, which, if compromised, might not just leave large areas without water (and for long periods), but most importantly may not reveal, or cover up for, the presence of impurities or of substances which are highly toxic and damaging to the health of citizens.

- hospital electronic systems: the electronic systems for managing patient’s clinical records could be compromised and/or, even worse, manipulated.

- electronic emergency management systems (such as the Italian 118 services and the fire brigade): this could cause a late response, or even the total lack of a response, to emergencies, with the result that the health and/or lives of one or more citizens would be put at risk.

- electricity grid management systems: the manipulation of these could represent the greatest threat thus far analyzed and, therefore, must be thought of as the absolute priority issue in terms of defending our nation.

It is enough to remind ourselves that without electricity, nothing would work: computers, trains, aircraft, hospitals, telecommunications services, supply systems, etc. This would most likely cause
a popular civil revolt, resulting in unmanageable damage to the Government’s image, and causing people to lose faith in it.

Also, in the event of a serious, targeted attack, and not a simple, temporary malfunction, there is little that the systems which control energy continuity could do to compensate for the system being compromised and for damage which could not be repaired within 24 hours, which would have the domino-effect of causing further blackouts as attempts were made to make up for the deficit in the supply of electricity.

In order to provide a complete overview, two further cases must be highlighted, in which at first glance it would seem possible that human lives could be put directly in danger. However, for two different reasons, this could not in fact occur. These two cases are:

- **railway electronic systems**, which, despite ‘taking on’ the locomotive as soon as the train arrives at the barrier at stations such as Rome or Milan and electronically managing its speed, time of arrival, and scheduling its route with respect to other trains on the same line and any stops to be made, are always subject to a procedure which means that overall control is never completely taken out of the hands of the driver of the train or the operator working within the train station control centre. These two operatives in fact, in a reciprocal, duplicate manner, control the operations undertaken electronically by the two computers (on the train and at the control centre), and are always, at any moment, able to manually intervene and override this automated process.

- **financial and banking systems**, which, in the same way as was explained with regards to the manipulation of the national electricity grid, despite not being able to cause the direct loss of human lives, control an asset so critical to the State that, at all times, they must be taken into direct consideration. The economic or financial collapse of an entire nation, in fact, could easily bring about public uprisings which would have a high risk of causing human lives to be lost.

In this particular case, however, most foreign countries would be reluctant to commit such a devastating act of cyberwarfare, given the fact that the financial collapse of one nation often has repercussions for many others. For this reason, nations which are normally considered to be ‘threats’ in terms of cyberwarfare - above all China and Russia - would not actually see any benefit from carrying out a massive electronic attack on these kind of systems, as they are already tightly ‘interconnected’, both economically and financially, to the Western world.
A different logic applies, however, to those economies which are particularly independent and shut off from the rest of the world, for example North Korea, which, conversely, might find an attack on Western financial systems to be highly convenient, given that, amongst other things, it would be immune from any possible counter-attack aimed at causing similar economic or financial damage. Seen this way, however, the strong influence that China currently exerts on that part of the world can be said to have a pacifying influence with regards to this particular threat – so much so, in fact, that we can say that such an event would be very unlikely to occur.
3.0 Data and statistical elements related to the threat

Currently, tracking down reliable data and statistics with which to support the theses so far put forward is a difficult, complicated activity.

This is true for two reasons: the first is linked to the – at least public - scarcity of data relating to acts of cyberwarfare and/or of a true, proper cyber-war; the second, on the other hand, is closely linked to what was previously mentioned in the introduction to this project with regards to the simplicity with which it is possible to cover up the true origin of any act/attack carried out using IT equipment, which is aimed at the computer systems of another State.

In any case, a good starting point can be tracked down in the document “Significant Cyber Incidents Since 2006”\(^\text{16}\), edited and updated by the Center for Strategic and International Studies, which collects and lists attacks which have been carried out on IT systems and the networks of Governments, defence departments and the largest high-tech companies, in addition to financial crimes which have caused losses of over one million dollars. Even a brief analysis of the contents of the list can shed light on how, in the short space of three years (2006-2009), there have been at least 44 attacks of this type, 30% of which occurred in 2009 alone\(^\text{17}\).

Further reflections can be made on data supplied by U.S. Strategic Command which, via the U.S.-China Economic and Security Review Commission\(^\text{18}\), has highlighted how over the course of 2008 the computer systems of the American Department of Defense registered 54,640 attacks on its computer systems. Furthermore, during the first six months of 2009, 43,785\(^\text{19}\) were recorded. Should the rate of these attacks remain constant, by the end of the year this would result in the annual number of attacks showing an increase of 60% with respect to 2008. A level of growth which was confirmed by the few statistical hints presented in the most recent Quadrennial Defense Review\(^\text{20}\), in which it was acknowledged that in the last two years computer attacks on the military sector have averaged over 5,000 per day, and also by the words of General Keith

\(^{16}\) This document, which was unfortunately only last updated on January 29 2010, can be found at the following address: [http://csis.org/files/publication/100120_CyberEventsSince2006.pdf](http://csis.org/files/publication/100120_CyberEventsSince2006.pdf)


\(^{19}\) In 2000, however, the number of IT incidents highlighted stood at just 1,415. It must be remembered, however, that this disconcerting increase is also in part due to the increased ability of the American Government to recognize these so-called cyber threats, and the growing attention world public opinion is giving to the subject.

Alexander – currently commander of U.S. Cyber Command – who, during the Senate hearing to confirm his nomination in April 2010, confirmed that the integrity of the computer systems of the Department of Defense are tested by those with malicious intentions “hundreds of thousands of times a day.” Surely the words of General Alexander refer to the so-called probing activities which are carried out on computer systems, and not to actual attacks, but this fact, should it come to be confirmed and supported by solid data, would certainly be revealing.

The American data, which is certainly substantial, seems however to lose a little of its consistency when compared to the recent declarations made by a representative of Azerbaijan’s State Protection Special Service, who, during an international workshop on the theme of “A Comprehensive Approach to Cyber Security”, revealed that the IT systems of critical Azerbaijani infrastructure are the targets of around 3,500 attacks every day, almost all of which come from Chinese and American systems, with around 15% also coming from Armenian systems. Certainly just as relevant is the fact that 3,060 computers are compromised daily on Australian soil, as is the fact that 6,039 cyber-incidents were recorded and confirmed by CERT-India in 2009, or the 1,942 intrusions observed up to August 2009 by the Malaysian Government.

---

22 According to the article “3,500 external penetrations fixed in state segment of Azerbaijani internet per day”, available at: http://abc.az/eng/news/47804.html
4.0 Conclusions

Before we are able to discuss any conflict conducted on that new battleground represented by the internet, and which is already dominated by the ‘fifth element’ after sea, land, air and space, we find ourselves today also having to fight a war of words over the meaning of the term ‘cyber-war’.

But what is a cyber-war? At what point can we say that we find ourselves facing an electronic war? What are its rules of engagement, and what methods are there for verifying that our responses are commensurate with any attacks suffered? Where can we lay the blame for any attack, and with what degree of certainty? When faced with the dangers that derive from a threat which, as much as it has been analyzed so far, certainly cannot be said to have been overestimated, these cannot and must not be thought of as simply academic questions.

Providing a convincing answer to these questions is not one of the objectives of this study, which is aimed more at providing evidence for, and developing, a debate on the real danger to human lives which even a single, isolated act of cyberwarfare, if well planned out, and/or a hypothetical cyber-war, could have. They are questions which, despite being posed at the very dawn of the creation of a specific Cyber Command by the American Department of Defense, have still not been answered definitively. They are also questions which are constantly being bandied about as part of this war of words between those who are convinced that the Western world – in primis America – has for some time been in the middle of a real cyber-war, and that it is losing it, and those who, despite the continuing and growing amount of criminal activity perpetrated over the internet, argue that the label ‘cyber-war’ was created for merely economic reasons by those hundreds of satellite companies which orbit the world of American Defense, and who are ready to try and ferment a fear of this new world (which is difficult for those who are not specialists in the subject to understand) in order to receive a share of the billions of dollars in consultancy fees set aside to help protect against this new threat.

Above all, the element which this debate (which already seems to be without end) seems to be missing is a solid understanding of the true nature of the threats originating from the internet. The term cyber-war is surely legitimate, but only when used to define those attacks carried out by military personnel using as their instruments computers or comparable electronic systems, and

---

which have as their targets the comparable computers, computer networks or electronic systems of their adversaries, with the intent of causing real-world damage.

This last point is the essential issue here: in order for us to be able to talk about cyber-war, it is necessary for those acts carried out using IT equipment to have had damaging consequences in the real, ‘offline’ world too. And this is the reason for which, for the majority of cases which until now have made it into the news, it is certainly more opportune to talk about acts of cyberwarfare, or acts which have as their objective the non-authorized violation of a computer in another country on its network or of any other activity which is part of an IT system by, or against, or supported by, a Government, which has the aim of adding, modifying or falsifying data, or to interrupt or damage, even temporarily, one or more networked devices, or any other device which is controlled by an IT system.  

And so, if what has been discussed above is correct, at this point it would be particularly difficult to describe this type of threat as having been ‘overestimated’, given the possibility (if not the probability) that the damage that might arise from this threat is not just verifiable, but that it could also put the lives of citizens in serious danger, as this study has shown.

---

28 This definition does not contain within itself the concept of “electronic espionage”, which, in many ways, is a completely different activity, at least on the theoretical, objective level, from that defined as cyberwarfare.
Biographical notes

Stefano Mele is a lawyer specializing in IT, privacy, security and intelligence law. He holds a PhD from the University of Foggia.

Stefano lives and works in Milan where he carries out consultancy work for large, often multinational, companies, on the subject of legal problems inherent within the issue of privacy and the protection of personal data, the internet and computer crime. He has prepared numerous publications and studies for books, reviews and specialist websites on these subjects.

He is also an expert in security, cyber-terrorism and cyberwarfare. He is a senior researcher at the Department of Strategic Intelligence and Security studies at the Link Campus University of Rome, and teaches the cyber-terrorism and cyberwarfare modules of its “Masters Degree in Intelligence Studies and National Security”.

He is a founding partner and vice president of the Centro Studi Informatica Giuridica di Foggia (CSIG-Foggia – ‘Foggia Centre for the Study of the Legal Aspects of Computing’) and is Sector Director ‘Intelligence and Electronic Espionage’ of the Italian Institute for Privacy.

The author thanks Davide Cardilli [http://www.theogre.org] for the cover design and layout of this document.