# Cooperation between Cyber Criminals and Terrorist Organizations

**Hergis Jica**

*PhD Candidate on National Security, Defence Academy "Spiro Moisiu", Tirana Albania*
*Master in Economic Sciences Thessaloniki, Grecce*
*Master in Penal Law Sciences Tirana, Albania*
*E-mail: hergisjica@hotmail.com*

**Doi:10.5901/mjss.2013.v4n9p532**

***Abstract***

*This paper examines some of the most widely researched trends and developments within the phenomenon of modern international terrorism, providing policy recommendations on how to counter its emerging threats in recognizing the strong impact of cyber criminals to terrorist organizations. The magnitude of the modern terrorist threat was demonstrated by the attacks of September 11, and ever since, the field has experienced a renewal of sorts, attracting unprecedented attention of all factors. This paper will address the meaning of the mutual need of cyber criminals and terrorist organizations and their mutual impact on state-nations. It will also present the many disciplines applicable to understand the combination of the traditional with the cybernetic, demonstrating that the phenomenon is multifaceted in nature, requiring a cohesive international and broad-based response. In covering a number of dilemmas deriving from the combination of these two groups, the paper explores the debate over a definition of cyber terrorism, providing a proposed definition that distinguishes the cyber terrorism from the cybernetic crime. The paper continues on to explore the phenomenon of modern cyber terrorism, the role of traditional crime within the cyber sphere, and the growing threat of cyber terrorism – including the cooperation between them, actions taken in the network, the help of cybernetic criminals etc. The role of cyber terrorism in democratic states and the economic ramifications of cyber terrorism are also explored. Finally, the paper ends with conclusions on how governments should see the cybernetic terrorism and the cybernetic crime, what should they understand about them and how immediate should be the answer to these new developments.*

***Keywords:*** *Cyber crime, Cyber terrorism, Attacks, International, Hacker, Cybernetic, Information, Cyberspace, Cyber threats, Cyber criminals, Organizations, Money, Virtual, State.*

## 1. Introduction

Today the world faces a wide array of cyber threats. The majority of these threats are aimed at the Western democracies and the Western-leaning countries of other regions. The reason is simple, because they are ripe targets, witch means that these countries have the right technology to enact "the game". These countries are either highly dependent, almost completely in some cases, on cyber means for nearly every significant societal interaction or are racing toward that goal. They seek the speed, accuracy, efficiency, and ease that a "wired" system of systems brings and all the benefits that accrue to such a situation.

The danger we face is that there are many individuals, groups, and states that desire to exploit those same systems for their own purposes. There is a new threat on the horizon that must be recognized and addressed.

Cyber threats we face today can be grouped into seven categories that form a spectrum of sorts. Any of these threat groups can attack an individual, a nation-state, and anything in between. They will exploit everything to reach the goal, beginning from an unprotected computer of a home user, an inefficient corporate information technology system, or a weak national infrastructure defense.

## 2. Levels of danger

We are all in danger from these threats, which can be grouped as low, medium, and high levels of danger. Any construct of this nature is a simplification, but it does aid in discussions to have the numerous possible actions defined into manageable groups.

At the low danger end, there are two groups of threats. The lowest level is the individual hacker. He operates for his own personal benefit: for pride, self-satisfaction, or individual financial gain. He constitutes an annoyance. The hacker

category also includes small groups who write malware (malicious software) to prove that they can or who attack small organizations due to personal or political issues.

With the hacker at the low end of the spectrum are small criminal enterprises and most disgruntled insiders. These too are low-level annoyances, except for the unfortunate individuals they exploit as their primary targets. These operate Internet scams, bilking people out of personal information, and may even perpetrate extortion through threats.

Continuing along the spectrum, the medium-level threats are harder to break down in a rank order. Each threat grouping targets different entities. These targets would consider their attackers very dangerous and a critical threat. These medium-level threats include:

- Terrorist use of the Internet;
- Cyber espionage, which is also helped by insiders at times, both corporate and national security types, including probes for vulnerabilities and implementation of backdoors; and
- High-level organized crime.

All three of these groupings can have extremely detrimental effects on a person, a business, a government, or a region. They occur regularly and define the ongoing significant threats we face every day.

The high-level threats involve the full power of nation-states. These come in two major groups. The first is a full-scale nation-state cyber attack.

The closest example is the example of Estonia, a sovereign state and a member of the Euro-Atlantic organizations, as usual today summarized by the political language we consume every day, bodies of European Community and NATO.

After the removal of the statue of the Soviet soldier from a park of the capital of Estonia, a massive attack on Estonia's information infrastructure, made these infrastructures to stop functioning, creating a total chaos in the state economy. This attack didn't use a very complicated "flooding" technique through the ghost computers (bootnets) on Estonian infrastructure, witch overloaded the network that way, that it couldn't withstand the load and ceased to exist.

The Estonian Minister of Defense, Jaak Aaviksoo, would declare for the "New York Times": "We're dealing with a situation that affects on national security, comparable with a situation when your ports are bombarded by the sea".

Major General Jonathan Shaw said the number of serious incidents was "quite small" but conceded it was likely that some attacks had gone undetected. In an interview with "The Guardian", Major General Shaw said the level of cyber attacks were "still on an upward curve", meaning increasing the security of the military's computer networks was now a top priority. "The number of serious incidents is quite small, but it is there," he said. "And those are the ones we know about. The likelihood is there are problems in there we don't know about". Major General Shaw said that next year's MoD budget was expected to include new money to improve cyber-defense despite widespread cutbacks. So, as above seen, this small country was sitting on his knees by such an event witch is very disturbing news for the future.

The other possibility is the cyber enablement of a kinetic attack before it occurs a traditional military attack by the move of the military troops. So far, we can only look to the assault on Georgia, dated on 08.08.2003. Georgia was not as dependent on the cyber realm as was Estonia, but the cyber assault that preceded the Russian military's ground attack into Ossetia severely hindered Georgia's response. Before and during the conflict, Georgia experienced an intense attack built on cyber attacks against government and civilian infrastructure network. Computer Network Operations (CNO), usually inherits a support function in military operations.

According to the United States, information operations doctrine, computer network operations, have several purposes, including denial, degradation or destruction of information in computer networks and data collection of the information in the system. Cyber attacks against Georgia showed similar functions. These attacks seemed to have different objectives, but most of the activities were targeted specifically to deny and terminate communication and therefore affected the overall flow of information within Georgia. Inability to dispose of information in a conflict can have serious psychological effects that can demoralize or disorientate people and decision-making authorities. But these attacks are not just designed to control the flow of information or to form a different perception of the people, they were also part of the active operations of extracting information, so, to steal and gather military and political intelligence from the Georgian networks. Although these attacks have used simple methods, they appeared to have been shot in a very sophisticated way that reached the desired goals successfully. Although Georgia has a relatively low number of Internet users and a lower overall dependency based on infrastructure, cyber attacks preceded and supported the general invasion that Russia initiated later.

## 3. A Construct for planning

During the Cold War and beyond, the military and security communities used a paradigm for planning that allowed them to determine against which of a large number of possible threats they should plan. They would determine both the *most dangerous threat* and the *most likely threat*. These were seldom the same.

During that period, there was near-universal agreement that full-scale thermonuclear exchange between the U.S. and NATO on one side and the Soviet Union and the Warsaw Pact on the other was the most dangerous threat. Fortunately, this was not the most likely threat, because, mutually assured destruction kept the fingers off the triggers.

But if you look nowadays, and make a brief comparison between the cold war and cyber war will see that considering the "cold war" transformed into "cyber war" is correct by having a new form of war global proportions. China and the U.S. both want a cyberspace based on rules, but do not see eye to eye. A Cold War, hosts potentially dangerous if they cannot agree on some rules of engagement. While cyber intensified competition between the U.S. and China in particular, the international community is approaching a crossroads. States can begin to control their online operations before things get out of control, to adopt a system based on rules governing cyberspace, and begin to respect each other's sovereignty virtual sovereignty of each other just as physical. Or, if the attacks and counter-attacks left unchecked, cyberspace may be the next country to a new Cold War for the Internet generation. Much of the old Cold War was characterized by indirect conflict involving forces of states parties, restarted in the 21st century of its history can become a virtual conflict pursued by mysterious players in the digital area.

While we face a scenario emerging from the cyber-threat spectrum that fully fits the part of the most dangerous threat, we must also face and prepare for a most likely scenario that is unique and, frankly, is not yet on the cyber-threat spectrum. This threat will involve the joining of the growing cyber-crime capability we see today with the terrorists' realization that the cyber realm is ripe for exploitation and that joining with cyber criminals will be their path to that exploitation.

## 4. The most dangerous Cyber Threat: Nation-State attacks

Clearly, as one looks at the spectrum of threats, the far end delineates the possibilities we fear most. Developed nation-states, acting as peer competitors, are the most dangerous potential threat.

Nation-states possess hard power, including kinetically capable militaries, economic strength, industrial bases, and scale of assets. They can marshal the intellectual capital to develop cyber armies--large numbers of operators with the best equipment, skilled at developing and using new forms of attack. These will do the twin tasks of both leveraging and enabling conventional intelligence, signals, and mobility assets.

Nation-states can also use their considerable coercive powers to harness civilian assets that technically fall outside the public sector. This can be done by requiring active or passive collusion with the government or by manipulating public sentiment to stir up patriotic fervor while providing guidance (i.e., targeting) and tools to the faithful.

All of the above factors allow nation-states with foresight to develop and use enormous capabilities in the cyber realm. What is today merely cyber espionage or probing of defenses can, in the blink of an eye, be turned into a massive attack on the infrastructure of an adversary.

Remember: Cyber forces do not need to deploy by ship, plane, or truck, so there are no logistical delays or the usual indicators and warnings. Cyber attacks could be used to disable defenses and blind intelligence capabilities in preparation for a devastating kinetic strike. These methods can slow the reactions of defenders by clouding their operation picture or fouling their communications means. Cyber attacks could bring down key command and control nodes altogether, paralyzing any response to the attack.

If the attacker has used weapons of mass destruction (chemical, biological, radiological, nuclear, and high-yield explosives) in the kinetic part of the attack, the cyber component can also hinder the ability to rally consequence-management assets. The victim will have suffered a catastrophic attack and will be unable to respond effectively to the results. The continued cyber intrusions will not only keep them from striking back with any real effect, but may make them ineffectual in mobilizing their first-responder forces. This kind of large-scale attack can only come from a nation-state and obviously constitutes our most dangerous scenario. It is very fortunate that it is also not a very likely one. The reason is old-fashioned deterrence. In the same way our cyber and physical infrastructures make us vulnerable to this scenario, any attacking nation-state must have its own infrastructure capabilities to be able to execute it. Those cyber capabilities and kinetic forces used in the attack are also potential targets, as is the remainder of the attacker's critical infrastructure.

Basically, it is unlikely that a nation-state would do this, because they also have much at stake. Deterrence, in the

same way we have understood it for over 50 years, still applies to nation-states in all the ways it does not apply to terrorists, criminals, and other non-state actors.

A large-scale cyber attack or cyber-enabled kinetic attack by a peer competitor on another country runs the risk of a large-scale response from the target or the target's allies and friends. While this will not dissuade every nation-state-backed cyber threat--the thousands of probes, minor attacks, and espionage actions prove that--it has continued and will continue to keep this type of nightmare scenario from moving into the "likely" category. Yes, we must prepare for it, but if this is the only thing we prepare for, we will have failed our countries.

One final thought on this subject: Opinion leaders might point to the situations in Estonia and Georgia mentioned earlier as evidence that deterrence did not work in 2007 and 2008. Friendly nations must explicitly state their intentions to protect and support one another from this sort of attack in the same way we did during the Cold War; without a strong declaratory policy of mutual defense in cyber situations, there will be no deterrence.

If we fail in this, smaller nations will continue to be at risk from larger, more powerful neighbors, and this is unacceptable. If we act strongly and in a united fashion, this will constrain nation-states--but will not constrain terrorists.

## 5. Terrorists and Cyberspace

It is fortunate that so far, the major terrorist organizations such as al-Qaeda and its franchises have not yet learned to fully exploit the "opportunities" in the cyber realm. But this doesn't mean it'll always be like this. In one of its interviews, Osama Bin Laden, has spoken regarding the possible constitution of a cyber army, by saying: *"hundreds of Muslim scientists were with him who would use their knowledge … ranging from computers to electronics against the infidels*".

Meanwhile, in April 2012, Al-Qaeda's main internet forums have been attacked, while they were offline for during the entire day, several others sites were downed weeks before, including two of the terrorist organization's top sites, al-Fida and Shamukh al-Islam.

At the moment there are no claims but the nature of the attacks suggests the intervention of groups of hackers hired by governments committed to the fight against terrorism.

Normally, it should be assumed that there will be commitment of these terrorist organizations in cyber war, for the fact that actors, are defining they roles quickly in this area. Most intelligence and law enforcement agencies agree that they are limited to such areas as communications, propaganda, financial dealings (fund-raising and fund transfers), recruitment, and intelligence. There is some potential use for operational planning and reconnaissance, but it is unconfirmed. Communications security on the Internet is very attractive to terrorists. The anonymity and difficulty of tracing interactions in restricted, password-protected chat rooms and the use of encrypted e-mails give terrorists a much greater degree of operational security than other means of communications. This will continue to be a major activity for terrorists over cyber channels.

Clearly, the terrorists are very good and getting better at using the Internet for propaganda and fund-raising purposes. The increasing sophistication of their messaging shows an understanding of the potential of the cyber medium in this area. They are reaching ever-increasing audiences.

YouTube-like videos, of terror attacks feed the fervor of the faithful around the world and make them feel a part of the struggle. Messaging over the Internet from the leadership keeps them prominent in the minds of the mass audience and makes the most isolated spokesperson seem relevant.

These same channels are superb for fund-raising among the dispersed peoples around the world. The reach and timeliness cannot be matched by other communications means and greatly aids in their fund-raising efforts. These same characteristics apply to their recruitment programs, and the process of radicalizing individuals no longer has to take place in person, but can be greatly enhanced by cyber communication and teaching.

There are many very effective applications available that aid in basic intelligence gathering. Google Earth and similar programs can be obtained for free and will give street-view photos of potential targets, as well as excellent route and obstacle information. The tendency of most Western countries to post nearly everything there is to know about critical infrastructures on unsecured Web sites is a great boon to the terrorists and requires no more expertise than an ability to use rudimentary search engines that small children have mastered. All of this "research capability" assists the terrorists in making their standard operation procedures much easier and safer to polish to a high degree.

A new wrinkle that is developing is the use of virtual worlds. There is hard evidence of money transfers having been made within these worlds. This is done by using real cash to buy virtual currency, conducting various transactions within the virtual environment, and then converting it back into real cash again in a completely different temporal location. It is all safe, clean, legal, and nearly impossible to trace.

These virtual worlds also allow for meetings to occur in cyber space that are even more deeply covered and protected than secure chat rooms. The avatars used in virtual worlds are very difficult to identify, and rules for interaction online allow for secret activities that further shield those with much to hide.

Someone must lead the terrorists of the world to the next level of cyber capability. It is unlikely that they will develop their own cyber plans and abilities beyond a few experts to ensure they are not being cheated or who can do operational cyber planning correctly. To do more than that would take a great deal of time, and they may be unwilling to wait. Unfortunately, they do not need to wait, as they will probably do it by reaching out to the world of cyber crime. There they will find willing partners to further their goals and plans, and these are definitely cybercriminals.

## 6. Cyber Criminals and Follow of the money

Cyber crime continues to be a booming business and continually adds new branches. What started as an offshoot of individual hackers doing it for fun and pride has grown into a huge (and still expanding) industry that steals, cheats, and extorts the equivalent of many billions of dollars every year. They steal from individuals, corporations, and countries. So, cyber crime is big money, and those who make possible the development of this industry, are cyber criminals. This industry, the more sophisticated it gets, the more organized it becomes, it has matured to a frightening level.

A lucrative target is data well beyond personal identity and financial information. Infiltrating businesses and stealing industrial secrets, pharmaceutical formulas, and like data can reap huge profits for criminals.

There are several reports of utility facilities having their SCADA (supervisory control and data acquisition) systems hacked and seized by criminals. The attackers have threatened to shut down the facility or worse if they were not paid enormous ransoms. No one knows if the malefactors could have actually followed through on the shutdown threats, as in each case the money was paid. The owners deemed it a credible threat and could not afford to have their enterprise closed or destroyed.

An interesting addition to this issue set is the illegal or quasi-legal franchising of cyber crime. Criminals now market and sell the tools of cyber crime. Root kits, hacking lessons, guides to designing malware, it is all available. These range from rudimentary "starter kits" to highly sophisticated programs that are potentially very destructive.

The last and, in my mind, most interesting and insidious threat is the rise of the botnets. Criminals cannot command entire nations of computers as one would expect that coercive governments could if they need to. Criminal syndicates have, however, developed huge botnets with members all over the world: members that they control without the actual owner of the machine even being aware of it. These zombie networks serve their criminal masters without question or hesitation. The criminals control them completely and can use them directly for DDoS (distributed denial of service) attacks, phishing, or malware distribution. They also rent them out to others for cash.

## 7. Terrorism enabled by Cyber Criminals

There is no doubt that terrorists want badly to hurt the modern Western and Western-leaning community of nations. The numerous dead and wounded, the horrific damage of past successful attacks, as well as the multiple foiled plots all make the deadly intent of the terrorists abundantly clear to all. This cannot be denied. Their continuing efforts to acquire and develop weapons of mass destruction for use against civilian targets is also *prima facie* evidence of this burning desire to do us harm in any way possible.

Terrorist organizations surely can find a number of highly trained, intelligent, and computer-literate people who are in agreement with their cause. These people can be taught to develop code, write malware, and hack as well as anyone. They cannot, in a timely manner, develop the kind of large-scale operational capabilities that a nation-state possesses. This is what they need to make a truly effective assault on the West in the cyber realm.

It is likely that there are two factors related to their activity and which can be:

- they do not really need to attack an entire nation to achieve success They desire to create a large event, but it does not necessarily need to be as extensive as a full nation-state attack
- they also have abundant funds and potential access to even more. These funds open up the criminal option, which will give the terrorists the capability to be extraordinarily destructive.

The West has a huge number of intelligence and law enforcement assets dedicated to stopping the proliferation of weapons of mass destruction. Any movement of these devices or materials related to them will sound the alarm across the world. Numerous arrests of people attempting to traffic in WMD or related materials have been made. This effort has nullified the effect of the excellent financial assets some terrorists have and frustrated their efforts to acquire WMD

capabilities. We do not have the same type of watchdog systems in place to prevent cyber enablement from occurring.

If a cash-rich terrorist group would use its wealth to hire cyber criminal botnets for their own use, we would have a major problem. A terrorist group so enabled could begin to overwhelm the cyber defenses of a specific corporation, government organization, or infrastructure sector and do much damage. They could destroy or corrupt vital data in the financial sector, cripple communications over a wide area to spread panic and uncertainty.

Related to this, we can very well take a look to an example dated on 28.03.2013 when the "American Express" website went offline for at least two hours during a distributed denial of service attack, by a terrorist organisation called "Cybernetic fighters of Izz ad-Din al- Qassam". This website was blocked from 3:00 p.m by a distributed-denial-of-service (DDoS) attack. In a statement, an "American Express" spokesperson said, "Our site experienced a distributed-denial-of-service (DDoS) attack for about two hours on Thursday afternoon...We experienced intermittent slowing on our website that would have disrupted customers' ability to access their account information. We had a plan in place to defend against a potential attack and have taken steps to minimize ongoing customer impact."

If terrorist organizations by cyber criminals will decide to carry out terrorist acts such as the destruction of the system of a nuclear plant then we would be in great danger, and yet if we think the same way, imagination what can be done, convinces us, that cyber capabilities that the criminals could provide would in short order make any terrorist organization infinitely more dangerous and effective.

Some have opinioned that cyber attacks are not suitable as terror tactics because they lack the drama and spectacular effect of, say, a suicide bomber. This does not take into account the ability of the terrorists to adapt. As our intelligence and law enforcement agencies continue to effectively combat the terrorists, they will continue to evolve. The terrorists' old methods will be augmented and improved. They will need to develop more imagination and versatility if they are to conduct successful operations.

Also, it should be taken into account the fact that since the terrorist organizations are lured by actions causing many victims or damages, than, normally, they'd be enticed, if, undisturbed, there would be a place in the world to press a button and see another consequence of the world that it would create. But we've to emphasize that if we'd combine a cyber terrorist attack with a traditional terrorist attack, the consequences would be unimaginable, tragedy and panic would be in the highest rate of such action.

Criminals, for their part, are motivated by greed and power. Few of the leaders of the enormous cyber organized crime world would hesitate at selling their capabilities to a terrorist loaded with cash. That fact, combined with the ever-growing terrorist awareness of cyber vulnerabilities, makes this set of scenarios not just likely, but *nearly inevitable*.

## 8. Conclusion

Terrorists will recognize the opportunity the cyber world offers sooner or later. They will also recognize that they need help to properly exploit it. It is unlikely they will have the patience to develop their own completely independent capabilities. At the same time, the highly developed, highly capable cyber criminal networks want money and care little about the source.

This is an inevitable connection and factor that makes this possible is the money. The threat of a full nation-state attack, either cyber or cyber-traditional together, is our most dangerous threat for the internal security. Deterrence, at all costs must be functional, but otherwise, there should be taken all possible measures to support protection.

Terrorists will never be deterred in traditional ways or by a lonely war of a nation-state. They will continue to seek ways to successfully harm us, and they will join hands with criminal elements to do so. A terrorist attack enabled by cyber crime capabilities will now be an eighth group of cyber threats, and it will be the most likely major event we will need to confront.

Some would say that cyber crime is a purely law enforcement issue, with no national security component. That is a dubious "truth" today if we see that. This is not a static situation, and it will definitely be more dangerously false in the future. Unless we get cyber crime under control, it will mutate into a very real, very dangerous national security issue with potentially catastrophic ramifications. It would be far better to address it now rather than in the midst of a terrorist incident or campaign of incidents against one of our countries. Terrorism, powered by network cyber criminals, is the biggest cyber threat, and to combat it, there should be used all the possible assets available.

## References

The New York Times, Digital Fears Emerge After Data Siege in Estonia, Mark Landler and John Markoff, Published: May 29, 2007 from web site: http://www.nytimes.com/2007/05/29/technology/29estonia.html, accessed date10.03.2013.

The Telegraph, Ministry of Defence computers hacked by cyber criminals, 04 May 2012, from web site: http://www.telegraph.co.uk/news/uknews/crime/9245273/Ministry-of-Defence-computers-hacked-by-cyber-criminals.html, accessed date 10.03.2013.

AFCEA International, The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict 24.05.2012, web site: http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf, accessed date 04.05.2013.

The Diplomat, Is Cyber War the New Cold War?, Trefor Moss, 19.04.2013, web site: http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/, accessed dt.05.05.2013

Security Affairs, Cyber terrorism, cyber attacks against al Qaeda 2.0, 06.04.2012, Pierluigi Paganini, web site: http://securityaffairs.co/wordpress/3986/cyber-crime/cyber-terrorism-cyber-attacks-against-al-qaeda-2-0.html, accessed date 06.05.2013.

http://www.youtube.com/results?search_query=cut+head+from+terrorist&oq=cut+head+from+terrorist&gs_l=youtube.3...5394.29770.0.31384.52.33.0.1.1.8.299.4397.9j15j7.31.0...0.0...1ac.1.11.youtube.9xnlL6Uxr-4, Main page, accessed date 04.05.2013.

Webopedia, SCADA, web site: http://www.webopedia.com/TERM/S/SCADA.html accessed date 02.05.2013.

Arstechnica, "Funded hacktivism" or cyber-errorists, AmEx attackers have big bankroll, Sean Gallagher, 30.03.2013, web site: http://arstechnica.com/security/2013/03/funded-hacktivism-or-cyber-terrorists-amex-attackers-have-big-bankroll/,accessed date 05.05.2013