THE INTERNATIONAL STRATEGY FOR CYBER SECURITY

[**Issue Number 102 - October 2017**](https://www.lebarmy.gov.lb/en/content/102-d)

**The international strategy for Cyber Security**  
Prepared By: COL. Eng. Robert Mansour  
Officer in the lebanese army

**Introduction**

Nowadays comparatively open and interoperable worldwide numerical infrastructure is being challenged in the form of cyber-attacks, ranging from minor malware to the whole existential crisis. The relationship between all concerned entities, as expressed by conventional or emerging cyber-attack styles and techniques, in a global cyber scene, is what we’ll refer to as “Universal Cyber Theatre” ahead. Hackers armed with bots, scripts, and unsavory methods of obtaining financial, intellectual, personal property or trade secret information continue to target businesses all over the globe.

Breaches to security can be ruinous, and can cost companies and nations a lot of money, time, and their standing. The dimensions of cyber have transformed key economic infrastructure and national assets into more attractive, high-value targets, while at the same time making them or rendering them more prone and vulnerable to significant threats.

The major threats arise from worldwide terrorism, nation-sponsored espionage and sabotage, and malevolent hacktivism. Any of these possibilities may involve the use of an “inner agent” to carry out or assist in the attack.

Every day, our digital identity is endangered by several cyber threats that are becoming even more sophisticated. Cyber criminals use millions of records, within data breaches exposed, that are used for illegal actions. Particular attention is given to medical records, technology secrets, tactical plans, financial records, or any specific type of data that is attracting the attention of the criminal ecosystem.

The Internet is universal. It connects many countries, and information generally flows freely across national borders. This characteristic raises remarkable policy concerns, not certainly directly concerned with security.

Day after day, it seems, a mammoth cyber-attack sponsored by a nation-nation comes to light. In recent years, more than 20 countries have announced their intent to launch or strengthen their offensive cyber capabilities. The result is an increasing digital arms race that presents a major threat to the security of our data. It is difficult, forensically, to distinguish nation-nation attacks from those of independent groups, even more so when China and Russia use nation hackers, and also pay freelancers when they gain access to useful systems. Among the intrigue and mystery, one thing is clear; the online world is becoming on increasingly unsafe place.([[1]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn1" \o "))

Novelties in technology are changing the tactics of modern-day conflict. There are new tools in today's arsenal of weapons. Helped by advances in electro-magnetic and modern information and communications technology, a new form of electronic warfare has been formed. It is called cyberwar, and is increasingly recognized by the governments and the military as posturing a potentially grave threat.

Using the internet as a platform for political action is one thing. But infiltrating and disrupting computer networks and databases take cyberwar to another level.([[2]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn2" \o "))

It has been called the “fifth dimension of warfare”. Along with land, sea, air and space, the cyber-world is increasingly becoming a new frontline. As cyber-attacks have neither limits nor borders, their effects on individuals, nations, or organizations, in addition to the tools of precautions and counter actions, should be highlighted.

**A. Problematic**

**First**: As cyber terrorism and cyber-crime, both are of major elements in cyber security, are no longer tied to a specific country; moreover, they have no boundaries, and have the ability to cross borders without the need of specific permissions.

**Second**: The lack of single international reference or body, like the International Criminal Court or the International Court of Justice to prosecute individuals, institutions, or countries that incite, help, contribute or get involved in such acts according to standard, national or international, provisions and penal laws.

**Third**: Lack of specialized judges or lawyers, specialists in the field of information technology, requires finding a solution to this dilemma to decide and judge on similar or relevant concerns.

**Fourth**: Allowance to use force and military action as a response or retaliation of cyber-attacks on a specific country, considering it as a military security, with international accordance, approval, and clearance.

**B. Scope**

The aim of the International Strategy for Cyber-Security is to provide a cohesive roadmap, initiatives, guidelines, and implementation mechanism for achieving the global vision on cyber-security, based on international and inter-agencies sharing and coordination, in accordance with a safe, secured, vibrant, resilient and trusted system, lawful and legal, that provides opportunities for its community, provides tools to minimize or eliminate cyber-crime and cyber-terrorism threats, safeguarding national assets and interests, promoting peaceful interactions and proactive engagement in cyber-space for national and international prosperity.

This strategy explores the idea of having a robust and solid cyber-ecosystem where the cyberdevices can operate with each other in the future to prevent cyber-attacks, reduce their effectiveness, or discover solutions to recover from a cyber-attack.

**Cyber World**

Originally, the internet goes back to the Cold War, and was mainly considered as a US military “command and control” network that could survive multiple nuclear attacks and retain communications and reactive capability.([[3]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn3" \o "))

Powered by the growth of cyber-space, the interconnection of critical infrastructure is growing, and with it some recognition of potential threats and vulnerabilities. But not everything is new or unusual. There are complicating and historical issues that interact with the current environment. In many ways, contemporary infrastructure threats look very different from those of the late 20th century, and it is important to be aware of these differences when designing adjustable response mechanisms.

Before the world had heard of Edward Snowden, before metadata, and before the surveillance program named Personal Record Information System Methodology (PRISM) under which the United States National Security Agency (NSA) collects internet communications from at least nine major US internet companies, and before encryption entered the banter of common conversation, so many countries such as China, Russia, North Korea, Iran, and even the United States government, organized crime groups, and became the seemingly everyday stuff of headline news.([[4]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn4" \o "))

Modern life is increasingly dependent on a multitude of interrelated and interdependent infrastructures. While sectors such as food, water, health, and transportation, and the infrastructure that supports them have always been critical, their ability to supply is increasingly trapped with the information and communications technologies that have become essential components of daily life.

Although cyber-space, the sum of these components, is sometimes categorized as an isolated sector, in practice it is so deeply embedded into sectors such as energy and transport as to make any separation meaningless. Cyber-space can be pictured instead as a thin layer or nervous system running through all other sectors, enabling them to communicate and function.

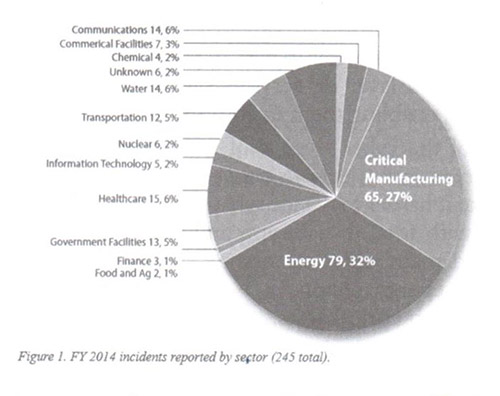
Security of the cyber layer is of great public importance, yet the compact interconnections between sectors, assisted by cyber-space, make it harder to decide what to protect. As transportation interlinks with food distribution and telecommunications, and as these and many other sectors are supported basically by the finance and energy sectors, it is more difficult to draw clear borders between critical areas.

This makes it difficult to counter evolving threats, which are rising along with dependencies. Dramatic yet hypothetical scenarios, such as acts of cyber-enabled terrorism, can’t be ruled out, but they overshadow the more ordinary but identifiable and persistent damage caused by organized crime and hacking.

This complex situation doesn’t reduce the responsibility of operators, owners, and service providers to secure their infrastructure. Potential vulnerabilities are revealed regularly and, although few of these are exploited on a large scale, and even fewer result in severe damage, the risk of disruption will continue to increase in parallel with growing connectivity.

Cyber-security is in many means an arms race between attackers and defenders Information and Communication Technology (ICT) systems are very complex, and attackers are continually searching for weaknesses, with the main vulnerabilities such as Insecure Communications, Information Leakage and Improper Error Handling, Broken Authentication and Session Management, Failure to Restrict URL Access, Cross Site Scripting, Code Mistakes, Untrained Users, and Insecure Configuration Settings.([[5]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn5" \o "))

The main identified vulnerable areas, as Fig.1 shows, could be as follows:

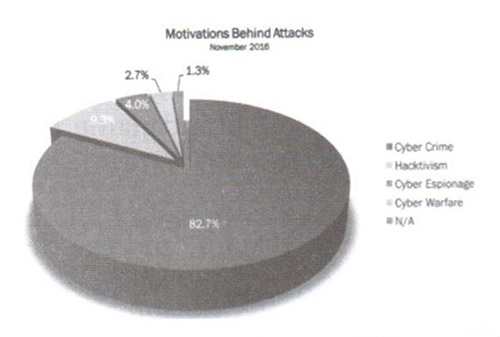


Internet-connected systems are attractive targets. The Internet is a critical infrastructure for national defense activities, navigation, transportation, energy resources, banking, finance, aviation, and necessary daily-life pursuits for billions of people. Major cyber-attacks have already occurred, for instance the Stuxnet worm([[6]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn6" \o "))and attacks in nations where mass opposition to a regime has taken to the streets. Cyber-attacks are an approaching and looming challenge for individuals and businesses, where governments, IT sectors, healthcare, communications, defense, chemical industry, and leaks among nations and persons as mentioned in what is perhaps the most well-known security breach, (former) U.S. Army Private Bradley Manning leaked hundreds of thousands of classified military and Nation Department documents to the WikiLeaks organization, which made many of them available on the Internet. WikiLeaks, the whistle-blowing organization, went live in 2006. Four years later, it released documents from the wars in Afghanistan and Iraq. These leaks of classified resources and materials have alarmed military leaders, businesses, and governments. So did WikiLeaks change cyber security measures?

The tale of WikiLeaks and its founder Julian Assange demonstrates how the U.S. should fight bad players in cyber-space. WikiLeaks has become a brand name for the disclosure of secrets of governments. But the more interesting and less widely remarked-upon part of the story concerns the reaction to Assange’s arrest in Great Britain, and the decision of many companies (including Amazon.com, MasterCard, and PayPal) to sever commercial and financial relationships with his Web site. Their response turned the WikiLeaks fiasco into a kind of cyber-war involving a non-nation group of commercial actors. The important decisions, however, had nothing to do with technology. They were tough calls made by corporate boards reacting responsibly to an unreliable and irresponsible act.([[7]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn7" \o "))Assange appealed to Ecuador for asylum in July 2012 at Ecuadorian embassy in London, after losing successive UK court battles to avoid extradition to Sweden and after the “threats” made by US officials that he could be arrested on espionage charges. Mr. Assange has not been charged with any crime till now, but there is an arrest warrant relating to the 2010 allegations.([[8]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn8" \o "))

People who perform cyber-attacks generally fall into different categories. The main ones are: criminals intent on monetary gain from crimes such as extortion or theft; spies intent on stealing proprietary or classified information used by private entities or governments; nation-nation warriors who develop capabilities and undertake cyber-attacks in support of a country’s strategic objectives; “hacktivists” who carry out or perform cyber-attacks for non monetary reasons; and terrorists who engage or get involved in cyber-attacks as a form of non-nation or nation-sponsored warfare.

As the figure below (Fig.2) shows, there are different motivations for cyber-attacks with different percentages.



The nature of attacks could be in different phases, such as Cyber Issues, Cyber-Crime, Cyber Terrorism, Cyber War, with different types of Attacks and Techniques.

And since technology has no set template or form, there are many different and various avenues of attack that a victim can fall susceptible to. Using software or hardware techniques and means, that are considered as basic risks and threats in the cyber-space theatre, as shown as per Fig. 3 below, the types of attacks that are listed beneath are just a short sampling of the tools of threats that exist:

• Malware (Metamorphic and Polymorphic)

• Viruses

• Spyware

• Worms

• Phishing

• Password Attacks

• Sniffing Attack

• Passive Attack

• Active Attack

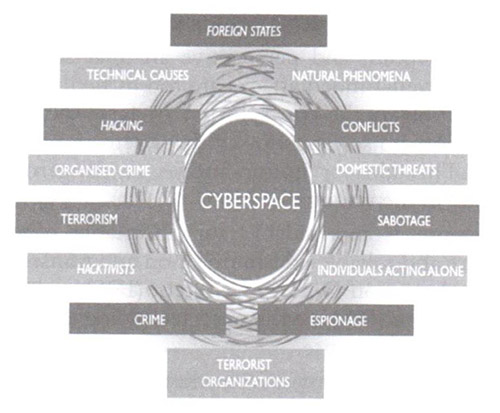
• Brute- Force Attacks

• Dictionary Attack

• Penetration

• Denial of Service Attacks

• Scam Attack



Today’s Cyber-Security Operations Centre (CSOC) should have everything it needs to mount a competent defence of the ever-changing information technology (IT) enterprise. The main strategies of effective CSOCs focus on consolidate functions of incident monitoring, achieving balance between size and visibility/agility, so that the CSOC can execute its mission effectively, giving the CSOC the authority to do its job through effective organizational placement and appropriate policies and procedures, favouring staff quality over quantity, realizing the full potential of each technology through careful investment, intense and keen awareness of, and compensation for, each tool’s limitations, and responding to incidents in a calm, calculated, and professional manner.

The basics of cyber and information security deals that provide insights into some of the complexities of cyber-security policymaking, where strategic imperatives are of main concern, include the risk cycle, including threats, vulnerabilities, and impact, in addition to the risks posed by software vulnerabilities.

**Not to forget that: Risk=Threats x Vulnerabilites**

The new viewpoint and perspective are that sophisticated, persistent and well-funded attacks are too difficult to prevent, making detection as the top priority. In fact, some security solution vendors go so far as to say that “detection is the new prevention”.This idea or notion moves us dangerously and unnecessarily in the wrong direction.

Cyber defense is unavoidable and inevitable in order to ensure secure and reliable communication and transmission of information. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are the main technologies dominating in the area of cyber defense.

Nowadays, cyber security is considered to be a critical and hot topic in national and international law, and very relevant and pertinent to international security discussions. Activity in domestic and cyber-space legislation with respect to it, must comply with the applicable and relevant international law.Within the aspect and realm of law applicable to and governing cyber activity, a host of legal regimes are relevant, including most notably national security law, domestic criminal law, and international law. This legal environment includes the Law of Armed Conflict (LOAC), the law governing the resort to force (jus ad bellum([[9]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn9" \o "))) and human rights law, along with domestic criminal law and national security law. Not to forget the role of International Court of Justice (ICJ), role of International Criminal Court (ICC), and role of International Criminal Police Organization (INTERPOL), where the Interference with a nation’s economic sphere, air space, maritime space, or territorial space, even if not prohibited by Article 2(4) of the UN Charter, is prohibited under the general principle of non-intervention. This fact is apparent in a number of treaties, UN Resolutions, and ICJ decisions that condemn coercion, interference, or intervention that falls short of the use of force. The ICJ has denoted and referred to some of this behaviour or conduct as ‘less grave forms’ of force that violate the principle of non-intervention while not triggering rights of a victim under Article 51.

Cyber Sabotage is yet becoming another new wrinkle in the emerging threats from cyber space. Cyber-theft or cyber espionage can result in exfiltration of proprietary, financial, or personal information from which the attacker can benefit, often without the knowledge of the victim. Denial-of-service attacks can prevent or slow legitimate users from accessing a system. Botnet malware can give the attacker command of a system for use in cyber-attacks on other systems.([[10]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn10" \o "))

As “cloud-streaming” fills our sky and “big data” gets bigger, digital assaults are destroying our digital devices at alarming rates. Cyber-attacks, natural disasters, international conflict, terrorism, and economic assaults are the top five global threats to international security. Cyber-assaults on the nation's critical infrastructure are on the rise at shocking and alarming rates.([[11]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn11" \o "))

A pool or collection of software robots, or “bots”, which creates an army of infected computers, known as ‘zombies', that are remotely controlled by the originator, send spam emails with viruses attached, spread all types of malware, and even can use any computer connected to the network as part of a denial of service attack against other networks or systems.

Attacks nowadays are based on high levels of threat intelligence (certainly, a very Sun Tzu styled approach([[12]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn12" \o "))).Threat intelligence is analyzed information about the opportunity, capability, and intent of malicious actors. As a type of intelligence, it is still performed through the intelligence lifecycle: plan, collect, process, disseminate and produce information. The key difference is that it’s focused on identifying threats. This information must be matched against an organization to determine if the threat intelligence is valuable to that organization.

At the same time, technological changes continue to disrupt how organizations compete and create value in ways which often change operating models. Among the explosion of data analytics, today’s most significant business trends, blending of service offerings across industries, and the digitization of business functions, to name a few, have expanded the use of data and technologies, and that is creating more risk than ever before.([[13]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn13" \o "))

Moreover, cyber-attacks are using the media as a primary tactic. But while the war of the near-future may well be fought in cyber-space, today's cyber-battleground of social media is already common and rife with conflict, one the West ignores at its own peril. These propaganda campaigns are savvy and sophisticated, forged from a deep knowledge of the target audiences and social media channels, and carried out with shocking and astonishing speed by an army of anonymous users spread across the globe.

Lately, social media platforms like Twitter, Instagram, and Facebook also have been used by the group fighters of Islamic Nation to coordinate and navigate their field operations on the ground. Additionally, social media has been used by Hamas to determine how effective missile strikes on Israeli targets are.

Moreover, social media is an efficient means of spreading misinformation, a tool that has been used in battles and wars for centuries. There are indications that Russia spends significant means and resources on misinformation campaigns targeting the United States. That pro-Putin online news article comment, mentioned below, may seem like it was posted by an American citizen, but may have been the work of a “Russian troll”.

In June 2015, Adrian Chen reported in New York Times that there are whole buildings in Russia filled with teams of employees who do nothing but feed the social media universe with misinformation. They even attempt to stir up horror and panic situations, like the time these trolls faked a chemical leak in a town in Louisiana, causing useless and needless alarm.([[14]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn14" \o "))

These kinds of actions can have wide and broad impacts. In 2013, the stock market dropped temporarily, and fear swept across social media after the Twitter account of the “Associated Press” was hacked and a “bogus and false tweet” reporting that the US president had been injured during a bomb attack on The White House. The nation-sponsored hacker group “The Syrian Electronic Army” claimed credit.

Whistleblower Edward Snowden has seized on a report that Russia is considering sending him back to the US as a “gift” to Donald Trump, saying that the story vindicates him of charges that he is a spy.([[15]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn15" \o ")) Edward Snowden’s leave to remain in Russia has been extended for three years, his lawyer has said, as a Russian official said the whistleblower would not be extradited to the US even if relations improved under the incoming president, Donald Trump.

Like it or not, social media is now the field or battleground where the targets are civilian. U.S. cyber-defense initiatives are presently, and perhaps rightly so, focused on more technically advanced threats such as theft of data, DDOS (distributed denial-of-service) attacks, or large-scale breaches. But social media requires no special skills other than the ability to communicate. Consequently, when social media becomes a battleground, the forces fighting there aren’t just made up of specially-trained soldiers, but of regular people, too.

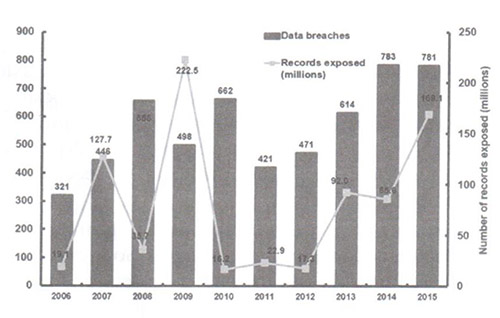
These forces are so great and distributed in numbers that any traditional battlefield analogy is meaningless. So as the U.S. Cyber Command is preparing the nation's defenses for the pending or coming ramp-up in cyberwarfare-like attacks, the messages spread instantly by groups of attackers through social media may not be receiving the attention they deserve.

To reverse this trend, the United Nations needs to be healthier at reaching the targets of misinformation campaigns than its adversaries, without breaching the privacy of those who needs protection. Authorities should search for ways to predict the publication or release of misinformation, and viral narratives should be neutralized before gaining momentum. The effort also would benefit from improved sharing of information between the private and public sectors, as well as between government entities.

Obviously, it seems that the United States is taking actions to prepare for a coming cyberwar. But it also seems that the United States has hardly begun erecting defences on the battleground of social media.

According to a report discussed by G20 summit that kicked off on Aug. 31th, 2016, in the Chinese city of Hangzhou, it was mentioned that there were over 85.5 billion cyber-attacks last year alone, which is more than 2,000 attacks each second.([[16]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn16" \o "))

As the following figure (Fig.4) shows, millions of attacks are recorded with data breaches.



These incidents were the starting signal to point over the fallouts of cyber security issues and how improper strategies could lead to disastrous situations.

In 1903, Nevil Maskelyne disrupted John Ambrose Fleming's public demonstration of Guglielmo Marconi's purportedly secure wireless telegraphy technology by sending insulting Morse Code messages through the auditorium's projector.([[17]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn17" \o ")) With the many malicious viruses and different types of aggressive malware out there today, it seems odd to think that just a few decades ago, at the birth of World Wide Web and other networks, security wasn’t always a top concern. In fact, in the very early stages of ARPANET, in 1969, a packet-switched network funded by the Pentagon, a number of intrusions were said to be made by high school students. The incidents continued, where the most notorious are as follows:

**1. The Original Logic Bomb(**[[18]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn18" \o ")**):**

**2. Moonlight Maze:**One of the earliest forms of major infiltration where hackers, willingly, penetrated American computer systems.

**3. Michael Calce:**Although Michael Demon Calce from West Island, Quebec, is just an ordinary 15-year-old boy, but in the cyber-space, he is very famous as ‘Mafia-Boy’.

**4. 4chan:**On October 1, 2003, Christopher Poole, a bored 15-year-old student from New York City, launched an English-language image board website used for posting pictures and discussion of the Japanese manga and anime, “4chan”.

**5. Titan Rain:** During 2004, Shawn Carpenter discovered a chain of coordinated “cyber raids”, where the FBI believed to be originated from government-supported cells in China.

**6. Sven Jaschan:** Sven Jaschan, who was a German college student confessed as the author of Sasser computer worms and Netsky worms, unleashed, in 2004 on his 18th birthday, a virus that had resounding effects all over the world.

**7. Operation Shady RAT:** In mid-2006, after an ongoing series of cyber-attacks started, Operation Shady Rat have hit at least 72 organizations worldwide, including the United Nations, the International Olympic Committee, defense contractors, and businesses.

**8. TJX:** On May 9th, 2007, TJX, a Massachusetts-based retailing company and owner of TJ Maxx and Marshalls, was just one of the many retailer companies hacked by Albert Gonzales and a group of hackers from the Shadowcrew.

**9. Hannaford Bros:** In 2007, Hannaford Bros, a grocery retailer, suffered a four-month long data-breach, wherein over 4.2 million debit and credit card numbers and other sensitive data were stolen by a group of hackers who installed malware on the stores’ servers, instead of the company’s databases.

**10. The Estonian Cyberwar:** On April 27th, 2007, the Estonian government was subjected to cyber terrorism by the Nashi, a pro-Kremlin group from Transnistria. Considered as one of the largest after Titan Rain, they employed a number of techniques such as botnets and ping floods to penetrate and take down key government websites rendering them useless.([[19]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn19" \o "))

**11. Project Chanology:**The largest protest movement against the Church of Scientology was led by Anonymous, a leaderless group of internet-based hacktivists, mainly originated from “4chan”.

**12. Presidential-Level Espionage:** During the 2008 presidency run, suspected hackers from Russia or China tried to attack the computer systems used in the campaigns of both Barrack Obama and John McCain that include sensitive data and emails used in the campaign. Because of the breach, the FBI confiscated all the electronic devices and all the computers; while many people hoped that the FBI would keep secret all the things they might dug up during the campaign trail.

**13. Heartland Payment System:** In 2008, the trusted payment processor Heartland Payment Systems fell into the trap set by Albert Gonzales of the Shadow-crew fame, that were responsible for phishing out over 100 million individual card numbers, costing Heartland more than $140 million dollars in damages.

**14.  July 2009 Cyber Attacks:**These were a series of coordinated attacks against major financial websites, government, and news agencies of both South Korea and the United States, involving the activation of botnet.

**15. Operation Aurora:** In 2009, it is a targeted malware attack, against at least 30 major companies, including Adobe and Google, which exploited a zero-day flaw in Internet Explorer.

**16. Stuxnet:**On June 2010, Iran was subjected to cyber-attacks when its nuclear facility in Natanz, was infected by Stuxnet, a cyber worm that was believed to be a combined effort of Israel and the United States, though no one claimed responsibility for its inception. The worm destroyed Tehran’s 1000 nuclear centrifuges, and set back the country’s atomic program by at least two years, due to its spread beyond the plant and infection over 60,000 computers as well.

**17. Canadian Government Hacking:** In February 2011, the Canadian government has revealed in news sources that they became a victim of cyber-attacks from foreign hackers with variable IP addresses from China.

**18. PayPal:** In December 2010, after PayPal permanently restricted the account used by WikiLeaks to raise fund, it became a victim of cyber-attack, citing their violation of the Acceptable Use of Policy as their reason. However, it did not only result in a series of multiple boycotts from individual users, but also caused hackers to move in.Thirteen people have pleaded guilty to charges connected to that 2010 cyber-attack.

**19. Epsilon:** Considered as the costliest cyber-attacks in history, the data breach in Epsilon, the world’s largest provider of handling services and marketing to industry giants such as Best Buy, JP Morgan Chase, and other major retailers and financial services, other major companies in 2011, has an estimated damage cost that ranged from $225 million to $4 billion dollars.

**20. Citigroup:** In 2011, over 200,000 - customer information, including contact details and account numbers,  were compromised resulting in $2.7 million loss for the company.

**21. Sony:** In 2011, an unknown group of cyber hackers stole 77 millions of PlayStation Network and Sony Online Entertainment accounts, including debit credit and card information users. The damage or outage from external intrusion was estimated at $1 to $2 billion dollars; and the worst issue that can happen to dedicated gamers happened, where hackers were able to log on, even when the company was trying to fix the breach that lasted for 24 days.

**22. Flame:** Flame is known as a modular computer malware that was discovered in 2012 as a virus used to attack computer systems in some countries in the Middle East that run on Microsoft Windows as their operating system. It is also known as Skywiper and Flamer.

**23. Opi Israel:** On April 7th, 2012, at the eve of Holocaust Remembrance Day, a coordinated cyber-attack by anti-Israel groups and individuals, DDoS assault that was timed for, with the aim of erasing Israel from the internet. Websites targeted by these hacktivists include non-profit organizations, educational institutions, financial and business sectors, newspapers, and privately owned businesses in Israel.

**24. Shamoon:** It’s a modular computer virus, that was used in 2012 in an attack on 30,000 Saudi Aramco workstations, causing the company to spend a week restoring their services.([[20]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn20" \o "))

**25. Red October:**Red October, which was discovered in 2012, was reportedly operating worldwide for up to five years prior to detection and discovery, transmitting information ranging from diplomatic secrets to personal information, including data from mobile devices.([[21]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn21" \o "))

**26. Gauss Trojan:** Being discovered in 2012, Gauss Trojan is a nation-sponsored computer espionage operation that uses nation-of-the-art software to extract a wealth of sensitive data from thousands of machines located mostly in the Middle East.([[22]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn22" \o "))

**27. CyberCaliphate:** On the evening of April 8th, 2015, TV5 Monde was the victim of a cyber-attack by the hacker group named "CyberCaliphate", which claimed to have ties to the terrorist organization Islamic Nation of Iraq and the Levant (ISIL). The hackers were able to breach the broadcaster's internal systems in what director Yves Bigot described as an "unprecedented" attack, overriding TV5 Monde's broadcast programming.([[23]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn23" \o "))

All these incidents were behind the rise of notable difficulties and debates to find a solution due to:

• Disability to Trace: Lately for example, the White House mentioned that President Putin had direct role in hacking US presidential elections,([[24]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn24" \o ")) but can this accusation be verified or traced easily?

• Lawful Tribunal Issues: Both the ICC and the ICJ outline the most serious crimes that would trigger the tribunal’s jurisdiction over individuals and nations, but they don’t include any Internet crimes or cyber-attacks that implicate human rights, and leave conspicuously absent any mention of freedom of speech.

• International Disorganization and Disagreements

• Globalization of Threats

• Non-Coordination of Security Organizations

• Lawful Concerns

• Private Sector Concerns

• Inter-government Agencies

• Sharing Cyber Information of Private Sector with the Government

• Regulatory Concerns

• Privacy Concerns

• Liability of Information

• Disagreement & Prevention of Cooperation within entities holding information

• Investigation Processes where there are some impediments, which obstruct police or security agencies investigations, digital forensics interrogations and prosecutions.([[25]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn25" \o "))

• Using Force in Response to Cyber-attacks: In 2011, when declaring “International Strategy for Cyber-space”, the White House announced that: “When warranted, the United States will respond to hostile acts in cyber-space as we would to any other threat to our country.

• Commercial and Business Roles

• Non Coherence of Technical Applications and Programs

• Lack of Expertise in IT among Judges and Investigators Impacts, Proposals, and Solutions

As there is no existing doctrine, organizational structure or physical infrastructure on how to integrate cyber-space operations into a multinational organization or international level, the international community started to go through multiple studies to face the challenges, starting from analysis of the problem, assessment of impacts, with effects, influences, consequences, and Cyber Protection Costs. Too many strategies and policies were set on national, regional levels, and international such as UN, ITU, IEEE, EU, OECD, NATO([[26]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn26" \o ")), thus resulting different standards such as ISO27001& ISO27002 according to the figure below:



All those strategies realize the importance of leveraging national resources and domestic potentials such as Computer Emergency Readiness Teams, Cyber Security Incident Response Teams, and Computer Incident Response Team (CERTs, CSIRTs, and CIRTs), since security threats today transcend borders, and thus require active international partnerships.([[27]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn27" \o "))

A “Road Map for Key Performance Indicators (KPIs) was essential for the process of building an international cyber-security strategy, mainly:

• Incident Reporting and Information sharing

• Institutional Arrangements for Cyber-security Bureaucracy

• Follow Standard Operating Procedures (SOPs), based on the following phases: Shape, Deter, Seize Initiative, Dominate, Stabilize, Enable Civil Authority.

The initial challenge in addressing current and future infrastructure cyber-security compliance strategy lies in cutting through the vast web of laws, regulations and the alphabet soup of inter-agency arrangements expected to play a role in the ever-evolving cyber-security space, putting in mind that proactively developing a targeted, comprehensive security plan that combines cyber and physical security measures is the key to placing every nation in the best posture to withstand government and public scrutiny in the event of a catastrophic cyber incident, because when it comes to critical cyber-security, the best defense is a good offense, based on the following objectives:

1. Protect the cyber-space essentials of each nation to reach global protection architecture;

2. Build and maintain ready actions and capabilities to conduct cyber-space operations relying on a solid core to provide the required services;

3. Set policies according to defined standards and reliable techniques, in accordance with relative private and public sectors;

4. Create scope of information sharing and interagency coordination to manage risks and optimize actions;

5. Set operational bridges to the private sector, including manufacturers, commercials, banks, and technology innovators;

6. Establish alliances, coalitions, unions, and partnerships to improve cyber actions levels and cyber-security plans;

7. Defend the global information network, secure nations’ data, and mitigate risks that could affect necessary missions;

8. Be prepared to defend each nation's vital interests from disruptive or destructive cyber-attacks of significant consequence;

9. Protect the local infrastructure and flow of information among continents and nations within secure environment;

10. Build and maintain viable cyber options, design and plan to use those options to control conflict escalation, and to shape the conflict environment at all stages;

11. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability;

12. Establish international reference entity with authoritative and legal chambers to take actions on the global level, with proper workforce and force tools for intervention purposes;

13. Build collaboration between the acquisition, intelligence, counter intelligence, law enforcement, and operations communities to prevent, mitigate, and respond to data loss;

14. Preventive and reactive national cyber-security capabilities should be built. Preventive measures require the development of national cyber-security policies, with an efficient compliance body that ensures the implementation of these policies. Reactive measures call upon the empowerment of a Computer Emergency Readiness Team (CERT), working in alignment with the national cyber-security strategy, and establish coordination with the international community.

The “Action Plan to Achieve Targets” focuses on:

1. Establishing an International Cyber-security Body.

2. Defining a National Cyber-security Strategy.

3. Establishing an International Dialogue.

4. Building Preventive National Cyber-security Capabilities.

5. Building Reactive National Cyber-security Capabilities.

6. Defining a National Talent Strategy.

7. Developing a Multinational Cyber-space Operations Doctrine.

8. Setting Actions of Negotiations.

9. Establishing Legal Framework.

10. Setting Legislative Options:

11. Establishing Coordination.

 The Solutions and Sustainable Implementations require:

1. Capability Process in order to provide end-to-end assured Cyber Network Operations (CyNetOps) with tools required to support, enable, or provide CyberOps capabilities to host-nation or other actors in order to contribute to attain cyber defense nation in depth.

2. Capacity Building.

3. Law Enforcement.

4. Establishing National-CyberPol.

5. Establishing Inter-CyberPol.

6. Establishing International Cyber-security Body.

7. Organizing Cyber-space Forces.

8. Establishing International Cyber Court.

This mission requires:

1. Legislations.

2. Regulatory Reform;

3. Technical and Technological Issues;

4. Cyber Risk Mitigation Model such as: System Characterization, Threat Identification; Vulnerability Identification, and Risk Assessment;

5. Supporting Development of Enterprises Providing Cyber-security and National Cyber-security Solution;

6. Enhancing the Fight against Cyber-crime;

7. Building Cyber Intelligence Platform;

8. Establishing International Channels of Dealing;

9. International Agreements;

10. Working on Next Generation Security Techniques and Strategic Initiatives applying:

**i. Technical Techniques Applied such as:**

• Accidental Internal Denial of Service Attack

• Training Methodology Principles

• Training By Doing

• Coaching – Training By Reorienting

• After-Action Reviews (AAR) – Training By Deconstructing

• Unannounced Exercises – Training Under Pressure

• Repeat Exercises – Training Through Repetition

**ii. Strategic Impact Initiatives aiming to:**

• Define capability;

• Benefit from nations’ initiatives, programs, and activities;

• Eliminate unproductive processes and bureaucracy;

• Measure Effectiveness;

• Access Differences among Institutions;

• Determine Relationships between Policy and Result;

• Streamlining;

• Standardization;

• Uniformity that contributes to efficiency;

• Monitor Progress toward Objectives;

• Being Proactive, not Reactive;

• Acting as a Catalyst, not Just a Passive Player;

• Apply Best Tools and Tactics;

These procedures will be faced by the following constraints:

1. Re-evaluation of Cyber-security Architecture;

2. Sovereignty of nations;

3. Nations’Vital Interests, Superpowers, and Influences;

4. Veto Power in Security Council;

5. Politics;

6. Budgeting;

7. Cyber Incident Management;

8. Establishing single point of authority;

9. Security vs Freedom;

10. Misuse of Power;

11. Cyber-wellness level;

**Conclusion**

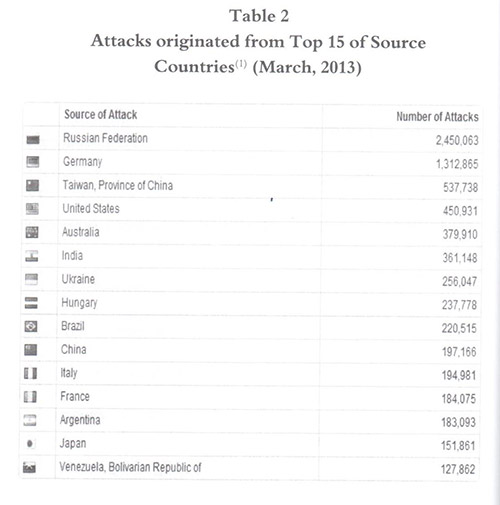
“Cyber-space is a new world where nations need to cooperate more than ever before”, as briefed by Federal Chancellor of Germany, Angela Merkel.([[28]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn28" \o "))

Cyber risk is now firmly at the top of the international agenda due to high-profile breaches that raise fears which hack attacks and other security failures could endanger the global economy.

Cyber security is one of the most urgent daily issues. Computer networks have always been the target of hackers and criminals, and it is expected that the danger of cyber security breaches will not only increase in the future as these networks expand, but there are sensible precautions that the world can take to minimize losses from those who seek to do harm.

With the right level of preparation and specialist external assistance, and with effective plan for sustainable strategy, it is possible to control damages, and recover from a cyber breach and its consequences. Benjamin Franklin([[29]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn29" \o ")) quoted:” If you fail to plan, you are planning to fail”.

Lastly, the criminal abuse of technology can be limited by providing proper tools, equipment, laws, global level of cooperation between nations (private and public sectors), and operational actions, then is the world safely prepared to face the future of technology. Eventually, as one author predicts, “the next world war will be fought with bits and bytes, not bullets and bombs”.([[30]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_edn30" \o "))



**REFERENCES**

**I. Books**

− Fred Kaplan,Dark Territory - The Secret History of Cyber War, Simon & Schuster Paperbacks, 2016.

− Richard Kissel, Glossary of Key Information Security Terms, 2013.

− Kenneth Geers, NATO Cooperative Cyber Defence Centre of Excellence, CCD COE Publication, 2011.

− Joanna F. DeFranco, What Every Engineer Should Know About Cyber Security and Digital Forensics, CRC Press, 2014.

− Thomas A. Johnson, Cybersecurity- Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, CRC Press, 2015.

− George K. Kostopolous, Cyberspace and Cyber-security, CRC Press, 2013, p.153.

− Arthur Appazov, Legal Aspects of Cyber-security, Faculty of Law, University of Copenhagen, 2014, p.4.

− Roderic Broadhurst, Investigating and Prosecuting Cyber Crime: Forensic Dependencies, Queensland University of Technology, 2006, pp. 408-433.

− Joanna F. DeFranco, What Every Engineer Should Know About Cyber Security and Digital Forensics, CRC Press, 2014, pp.15-21.

− Thomas A. Johnson, Cybersecurity- Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, CRC Press, 2015, p.255.

− Kenneth Geers, NATO Cooperative Cyber Defence Centre of Excellence, CCD COE Publication, 2011, p.17.

− Richard Bejtlich, Strategic Tools in Cyberspace: Beyond Tools and Tactics, 2015, Chapter 18, p.162.

**II. Reports and Documentations**

− UN General Assembly, Creation of a Global Culture of Cyber-security and the Protection of Critical Information Infrastructures, UN document A/RES/58/199, 30 January 2004.

− UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/65/154, 20 July 2010.

− UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/66/152, 15 July 2011.

− UN General Assembly, Letter Dated 12 September 2011 from Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN document A/66/359, 14 September 2011.

− US Army Capabilities Integration Center, Local Effects for Local Commanders Concept of Employment (CONEMP) of Cyberspace Capabilities at the Tactical Level, 2014.

− The International Committee of the Red Cross, International Humanitarian Law, 31 December 2006.

− Council of Europe, The Convention on Cyber-crime, also known as The Budapest Convention on Cyber-crime or The Budapest Convention, ETS No.185, 2001.

− UN General Assembly, Combating the Criminal Misuse of Information Technologies, UN document A/RES/56/121, 23 January 2002.

− UN General Assembly, Creation of a Global Culture of Cyber-security and the Protection of Critical Information Infrastructures, UN document A/RES/58/199, 30 January 2004, p. 2.

− UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/65/154, 20 July 2010; General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/66/152, 15 July 2011.

− UN General Assembly, Letter dated 12 September 2011 from Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN document A/66/359, 14 September 2011, p. 4.

− US Army, Local Effects for Local Commanders Concept of Employment (CONEMP) of Cyberspace Capabilities at the Tactical Level, by US Army Capabilities Integration Center, 2014, p.5.

**III. Magazines, Journals, and Newspapers**

− William Stahl, Georgia Journal of International and Comparative Law, 2011.

− Satola & Judy, William Mitchell Law Review, 2011.

− Nicole Perloth, Cyberattack on Saudi Firm Disquiets U.S., New York Times. pp. A1. Retrieved October 24, 2012.

− Dan Goodin, Massive espionage malware targeting governments undetected for 5 years,January 14, 2013, Ars Technica, Retrieved November 8, 2014.

− Dan Goodin, Nation-sponsored malware with Stuxnet ties has mystery warhead, August 9, 2012, Ars Technica, Retrieved November 8, 2014.

− Daily Telegraph,Isil hackers seize control of France's TV5Monde network in 'unprecedented' attack, 9 April 2015, Retrieved 10 April 2015.

− B. Hoyte, The need for Transnational and Nation-Sponsored Cyber Terrorism Laws and Code of Ethics, 2012.

**IV. Websites**

− Wired Magazine, https://www.wired.com/2015/09/cyberwar-global-guide-nation-nation-digital-attacks/.

−  Computer Hope, http://www.computerhope.com/jargon/s/scam.htm.

− CNN, http://edition.cnn.com/2014/12/19/politics/government-hacks-and-security-breaches-skyrocket.

− eSecurity Planet, http://www.esecurityplanet.com/network-security/health-care-industry-susceptible-to-cyber-attacks.html

− Computer Hope, http://www.computerhope.com/jargon/s/scam.htm.

− Federation of American Scientists, http://www.fas.org/sgp/crs/misc/R43831.pdf.

− InfoSec Institute, http://resources.infosecinstitute.com/risks-cyber-threats-healthcare-industry/.

− InfoSecurity Group, http://www.infosecurity-magazine.com/news/banks-hit-300-times-more-attacks.

−The Royal Society of Chemistry, http://www.rsc.org/chemistryworld/2015/06/chemical-plants-vulnerable-cyber-attacks.

− The Heritage Foundation, http://www.heritage.org/research/reports/2011/05/lessons-of-wikileaks-the-us-needs-a-counterinsurgency-strategy-for-cyberspace.

− TIME, http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare.

− ICRC, International Committee of the Red Cross, https://www.icrc.org/en/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum.

− Tripwire, The Nation of Security, http://www.tripwire.com/nation-of-security/security-data-protection/cyber-threat-intelligence/.

− The Global Nation of Information Security Survey 2016, http://www.pwc.com/gsiss.

− Research and Development, http://www.rand.org/blog/2015/07/war-on-the-web.html

−Defensetech, http://www.defensetech.org/2008/02/06/cyber-sabotage/.

−Digital Assaults are Defeating our Digital Devices, https://www.linkedin.com/pulse/20140613174410-90103575-digital-assaults-are-defeating-our-digital-devices.

−CCTV AMERICA, http://www.cctv-america.com/2016/08/31/research-institutes-release-g20-cyber-security-trend-report.

−The History of cyber Attacks, Jonathan Zheng, https://prezi.com/2qhwnmzdelcx/the-history-of-cyber-attacks/.

−Cyber Warfare and Terrorism, https://rconnon12.wordpress.com/2014/10/26/third/.

−Netherlands Institute of International Relations, http://www.clingendael.nl/sites/default/files/Clingendael\_Policy\_Brief\_Foreign%20Policy%20Responses\_September2015.pdf.

−Software Engineering Institute, Tracking and Tracing Cyberattacks, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5831.

−The Guardian, https://www.theguardian.com/world/2016/dec/15/white-house-putin-russia-hacking-us-election-trump.

−Archive of European Integration, Andrea Renda, http://aei.pitt.edu/42910/1/AR\_Cybersecurity.pdf.

−Just Security, George Eichensehr, International Agreements and Disagreements on Cyber-security, 2014, https://www.justsecurity.org/16706/international-agreements-and-disagreements-on-cyber-security/.

−Information Technology Industry Council, https://www.itic.org/dotAsset/2962f7a8-5b34-4729-bd8f-94cdbf29ebd3.pdf.

−International Journal of Cyber Criminology Vol 9 Issue 1 January – June 2015, http://www.cyber-crimejournal.com/Brown2015vol9issue1.pdf.

−International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World’ (May 2011), http://www.whitehouse.gov/sites/default/files/rss\_viewer/international\_strategy\_for\_cyberspace.pdf.

−The Guardian, https://www.theguardian.com/technology/2015/nov/14/hackers-technology-bounty-discover-flaws.

−Reuters, http://www.reuters.com/article/us-china-ransomware-idUSKCN0WG2L5.

−Congressional Research Service, Cyber Security Issues and Challenges, August 12th, 2016, www.crs.gov.

−BBC, the former "leader" of hacking group, http://www.bbc.com/news/technology-27579765.

−The White House, https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact\_sheets/cyber-security.pdf.

−Security Intelligence, https://securityintelligence.com/news/pwc-preview-banks-cyber-security-budgets-go-big/.

−The National Strategy to Secure Cyberspace, https://www.us-cert.gov/sites/default/files/publications/cyberspace\_strategy.pdf.

−GOV.UK, https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary.

−Office of the Minister of Nation for Administrative Reform, http://www.omsar.gov.lb/cyber-securitypolicy/.

−ITU National Cyber-security Guide, http://www.itu.int/ITU-D/cyb/cyber-security/docs/ITUNationalCyber-securityStrategyGuide.pdf.

−IEEE Xplore, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6246114.

−IEEE USA, https://www.ieeeusa.org/policy/whitepapers/IEEEUSAWP-RiskingitAll2014.pdf.

−European External Action Service, http://eeas.europa.eu/enp/documents/2015/151118\_joint-communication\_review-of-the-enp\_en.pdf.

−PwC’s Strategy&, http://www.strategyand.pwc.com/reports/cyber-security-middle-east.

−NATO, http://www.nato.int/cps/en/natohq/topics\_78170.htm.

−British Standards Institution, http://www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/Standards-for-IT-and-cyber-security/.

−ISA Security Compliance Institute, http://www.isasecure.org/en-US/.

−Tripwire, The Nation of Security,http://www.tripwire.com/nation-of-security/government/a-comparative-analysis-of-national-cyber-security-strategies-germany-and-the-u-s/.

−ESET Security Community, http://www.welivesecurity.com/2016/09/01/financial-cyber-security-needs-key-agenda-item-g20/.

−ITU, http://www.itu.int/ITU-D/cyb/cyber-security/docs/ITUNationalCyber-securityStrategyGuide.pdf.

−The MITRE Corporation, https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf.

−Federation of American Scientists, https://fas.org/irp/doddir/army/pam525-7-8.pdf.

−US Army Cyber Command, www.arcyber.army.mil/Organization/NETCOM.

−Tech Target Network, http://searchsecurity.techtarget.com/feature/Cyber-security-professionals-Five-ways-to-increase-the-talent-pool.

−2001 Budapest Convention on Cyber-crime, http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

−Law Enforcement Cyber Center, http://www.iacpcybercenter.org/#sthash.GP2B0xyx.dpuf.

−Human Rights Brief, http://hrbrief.org/2012/12/international-criminal-tribunal-for-cyber-crime-and-human-rights/.

−The White House, https://www.whitehouse.gov/sites/default/files/rss\_viewer/international\_strategy\_for\_cyberspace.pdf.

−European Union Agency for Network and Information Security, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia\_Cyber\_security\_Strategy.pdf.

−UN, https://www.un.org/disarmament/wmd/nuclear/.

−RAND Corporation, http://www.rand.org/blog/2015/09/define-acceptable-cyberspace-behavior.html.

−System Administration Networking Security Institute, https://www.sans.org/reading-room/whitepapers/bestprac/practical-cyber-security-training-techniques-support-employees-34267.

−The White House, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

−The Future of Smart Cities, https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf.

−World Bank, http://siteresources.worldbank.org/INTBELARUS/Resources/M&E.pdf.

−PwC Netherlands, https://www.pwc.nl/nl/assets/documents/pwc-brochure-cyber-security.pdf.

−Center for Strategic and International Studies, https://csis-prod.s3.amazonaws.com/s3fs-public/130208\_Lewis\_ConflictCyberspace\_Web.pdf.

−Investment Industry Regulatory Organization of Canada,http://www.iiroc.ca/industry/Documents/CyberIncidentManagementPlanningGuide\_en.pdf.

−ITU & ABI Research, International Telecommunication Union, http://www.itu.int/dms\_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

−Cooperative Cyber Defense Centre of Excellence,https://ccdcoe.org/AngelaMerkel.html.

−InterPol, www.interpol.int/content/download/773/6131/version/5/file/agn72r01.pdf.

−Forensic Focus,http://articles.forensicfocus.com/2012/09/28/the-need-for-transnational-and-nation-sponsored-cyber-terrorism-laws-and-code-of-ethics.

−Infosec Institute, http://resources.infosecinstitute.com/risks-cyber-threats-healthcare-industry.

−Deutsche Telekom Cyber Initiative, http://www.cfr.org/councilofcouncils/global\_memos/p32414.

−Kaspersky, https://usa.kaspersky.com/internet-security-center/threats/trojans#.V0W\_HY9OLmI.

−National Cyber-Security Institute, http://www.nationalcyber-securityinstitute.org/editorials/what-does-cyber-security-have-to-do-with-our-food-supply/.

−Ministry of Transport and Communications,http://www.motc.gov.qa/en/documents/document/national-cyber-security-strategy.

−The National Security Strategy – Enisa, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS\_ESen.pdf

−Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx.

−German Federal Bureau of Interior, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber\_Security\_Strategy\_for\_Germany.pdf?\_\_blob=publicationFile.

−OECD, http://oe.cd/security.

[[1]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref1" \o ")https://www.wired.com/2015/09/cyberwar-global-guide-nation-state-digital-attacks/, access date: 10/06/2016.

[[2]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref2" \o ") Aljazeera, http: //www.aljazeera.com/ programmes/ aljazeeraworld /2011/10/2011101916939402528.html, access date: 20/06/2016.

[[3]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref3" \o ") Johnny Ryan, ‘How the atom bomb helped give birth to the Internet’, ars technica, 21 February 2011, http://arstechnica.com/techpolicy/ 2011/02/how-the-atom-bomb-gave-birth-to-the-internet/, access date: 16/05/2016.

[[4]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref4" \o ") Fred Kaplan, Dark Territory - The Secret History of Cyber War, Simon & Schuster Paperbacks, 2016, p.319.

[[5]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref5" \o ") Federation of American Scientists, http://www.fas.org/sgp/crs/misc/R43831.pdf, access date: 23/8/2016

[[6]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref6" \o ") Stuxnet, a joint U.S.-Israel project, is known for reportedly destroying roughly a fifth of Iran’s nuclear centrifuges (Natanz nuclear facility) by causing them to spin out of control.

[[7]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref7" \o ") The Heritage Foundation, http://www.heritage.org/research/reports/2011/05/lessons-of-wikileaks-the-us-needs-a-counterinsurgency-strategy-for-cyberspace, access date: 29/05/2016.

[[8]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref8" \o ")http://www.telegraph.co.uk/news/worldnews/wikileaks/11681502/Why-is-Julian-Assange-still-inside-the-embassy-of-Ecuador.html, access date: 21/9/2017.

[[9]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref9" \o ") International Humanitarian Law, published by the International Committee of the Red Cross, https://www.icrc.org/en/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum, access date: 19/06/2016.

[[10]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref10" \o ") Defensetech, http://www.defensetech.org/2008/02/06/cyber-sabotage/, access date: 14/06/2016.

[[11]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref11" \o ") Digital Assaults are Defeating our Digital Devices, https://www.linkedin.com/pulse/20140613174410-90103575-digital-assaults-are-defeating-our-digital-devices, access date: 14/06/2016.

[[12]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref12" \o ") THE STATE OF SECURITY, http://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/, access date: 13/06/2016.

[[13]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref13" \o ") Ibid.

[[14]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref14" \o ") Research and Development, http://www.rand.org/blog/2015/07/war-on-the-web.html, access date: 08/06/2016.

[[15]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref15" \o ")https://www.theguardian.com/us-news/2017/feb/10/edward-snowden-russia-trump-report, access date:21/09/2017.

[[16]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref16" \o ") CCTV AMERICA, http://www.cctv-america.com/2016/08/31/research-institutes-release-g20-cyber-security-trend-report, access date: 05/09/2016.

[[17]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref17" \o ") Jonathan Zheng, The History of Cyber Attacks, https://prezi.com/2qhwnmzdelcx/the-history-of-cyber-attacks/, access date: 16/05/2016.

[[18]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref18" \o ") Cyber Warfare and Terrorism, https://rconnon12.wordpress.com/2014/10/26/third/, access date: 21/06/2016

[[19]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref19" \o ") Netherlands Institute of International Relations, http://www.clingendael.nl/sites/default/files/Clingendael\_Policy\_Brief\_Foreign%20Policy%20Responses\_September2015.pdf, access date: 18/05/2016

[[20]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref20" \o ") Perloth, Nicole (October 24, 2012). "Cyberattack On Saudi Firm Disquiets U.S.". New York Times. pp. A1. Retrieved October 24, 2012.

[[21]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref21" \o ") Dan Goodin (January 14, 2013). "Massive espionage malware targeting governments undetected for 5 years". Ars Technica. Retrieved November 8, 2014.

[[22]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref22" \o ") Ibid, (August 9, 2012). "Nation-sponsored malware with Stuxnet ties has mystery warhead". Ars Technica. Retrieved November 8, 2014

[[23]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref23" \o ") "Isil hackers seize control of France's TV5Monde network in 'unprecedented' attack". Daily Telegraph. 9 April 2015. Retrieved 10 April 2015, access date: 20/05/2016.

[[24]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref24" \o ") The Guardian https://www.theguardian.com/world/2016/dec/15/white-house-putin-russia-hacking-us-election-trump, access date: 17/12/2016.

[[25]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref25" \o ") International Journal of Cyber Criminology Vol 9 Issue 1 January – June 2015, http://www.cyber-crimejournal.com/Brown2015vol9issue1.pdf, access date: 15/08/2016.

[[26]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref26" \o ") Kenneth Geers, NATO Cooperative Cyber Defence Centre of Excellence, CCD COE Publication, 2011, p.17 www.ccdcoe.org.

[[27]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref27" \o ")http://www.tripwire.com/state-of-security/government/a-comparative-analysis-of-national-cyber-security-strategies-germany-and-the-u-s/, access date: 05/10/2016.

[[28]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref28" \o ") Cooperative Cyber Defense Centre of Excellence, https://ccdcoe.org/AngelaMerkel.html, access date: 27/08/2016.

[[29]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref29" \o ") Benjamin Franklin, 1706-1790, was one of the Founding Fathers of the United States. Franklin was a leading author, printer, political theorist, politician, freemason, postmaster, scientist, inventor, civic activist, statesman, and diplomat.

[[30]](https://www.lebarmy.gov.lb/en/content/international-strategy-cyber-security" \l "_ednref30" \o ") B. Hoyte, The need for Transnational and State-Sponsored Cyber Terrorism Laws and Code of Ethics (2012). Available at http://articles.forensicfocus.com/2012/09/28/the-need-for-transnational-and-state-sponsored-cyber-terrorism-laws-and-code-of-ethics (29 December 2012).

**الاستراتيجية الدوليّة للأمن السيبراني**  
مع التطوّر التقني في أنظمة وشبكات المعلوماتيّة نتيجةً للعولمة التي اجتاحت الكرة الأرضيّة، أصبح هذا العالم دون حدود جغرافيّة، ولا وجود معابر لشبكات تبادل المعلومات، مما أدّى إلى امكانيّة اختراق الدول والحواجز، من دون الحاجة إلى سمات دخول، وبالتالي الوصول إلى الخصوصيات والولوج إلى المواقع المحصّنة، فأصبح العالم "مسرحًا" لشبكات المعلوماتيّة، عناصرها المستخدمين ومحرّكات الإبحار والتطبيقات، فنتج عنها عناصر وعوامل مستجدّة منها الإرهاب الإلكتروني، الجريمة الإكترونيّة، استخدام مواقع التواصل الإجتماعي لنشر الإشاعات وبثّ الأخبار المضلّلة، إضافةً للتعرّض إلى شبكات المصارف، العبث في قواعد البيانات العائدة للمؤسسات، وزارات الدفاع، الأجهزة الأمنيّة، الملفات الطبيّة وغيرها، فأصبح مجال هذه الشبكات هو البعد الخامس للحروب، إضافة إلى الأبعاد القائمة في البحر، الجو، اليابسة، والفضاء الخارجي.  
خلال السنوات الماضية، حصلت عدّة اختراقات وهجومات إلكترونيّة كعمليّة "أورورا" في العام 2009 التي أدّت إلى تعطيل وتبدبل في معطيات ومعلومات مواقع "غوغل" و"أدوبي"، اعتداء "Stuxnet" في العام 2010 الذي أدّى إلى أعطال في شبكات المفاعل النووي الإيراني، وثائق "Wikileaks" التي هُرِّبَت واستخدمها مؤسس الموقع "جوليان أسانج"، الوثائق التي هرّبها "ادوارد سنودن"، الهجوم الإلكتروني المنظّم من قبل الدولة الإسلاميّة في العام 2015 على مواقع إخباريّة عالميّة، بالإضافة إلى فيروس "واناكراي WannaCry" في أيار 2017 الذي ضرب العديد من الشركات والمصارف العالميّة، وهنا تطوّرت ظاهرة "Hackers" أي "قراصنة المعلوماتيّة".  
وفق إحصاءات المنظمات الدوليّة العاملة في هذا المجال، بلغ عدد محاولات الإختراق خلال شهر آب 2017 أكثر من أربعة ملايين وستماية ألف محاولة، أدّت إلى خسائر تجاوزت مليارات الدولارات، مما دفع الدول الكبرى إلى تخصيص مبالغ تتعدّى التريليون دولارًا أميركيًا للفترة الممتدّة حتى العام 2021 لإنشاء أنظمة الحماية. وقد تبيّن أن أهمّ أسباب هذه الخروقات تعود إلى ضعف إجراءات الحماية والوقاية، ضعف وسائل الحماية، عدم وضع سياسات ومبادىء لأمن الشبكات والردود المناسبة، ازدياد مستوى وشموليّة التهديدات وعدم القدرة على تحديد مصدر الإختراق، فكانت النتائج السلبيّة التي أدّت إلى توقّف شبكات وأنظمة المعلوماتيّة، سرقة المعلومات والبيانات، استخدام وسائل الإبتزاز، وتبديل في مضمون المعلومات. إضافة إلى ذلك، برز موضوع العالميّة لاختراق الشبكات، فإذا كان هناك مواطنًا "لبنانيا" مقيمًا في استراليا، لديه عنوان بريدي وبوابة إلكترونيّة مسجّلة في استراليا واستخدم الشبكات الإفتراضيّة وأطلق اعتداء"إلكترونيًا" على هيئة أمنيّة في اوكرانيا، فكيف تتم المعالجة ولمن تُقدّم الشكوى؟ الاعتداء حصل من لبنان تحت عنوان إلكتروني مصدره استرالي!...  
من هنا برز موضوع "الأمن السيبراني" أو "أمن المعلومات"، نتيجة لذلك كان لجوء الدول والمنظمات الدوليّة والإقليميّة إلى وضع استراتيجيات وطنيّة لسياسات الحماية ومبادىء التصرف والتدخل، والحد من المخاطر، حتى أنّ البعض وضع استراتيجية تسمح باستخدام القوة والسلاح كما حصل في استراتيجية الولايات المتّحدة التي أطلقها الرئيس أوباما، مما أدّى إلى إشكاليّة دوليّة كونها تتعارض مع مبادىء وبنود ميثاق الأمم المتحدة، لا سيّما المادة 51 التي تقرّ بامكانية الردّ المسلّح فقط في حال الاعتداء المسلّح.  
في حالات الجرائم والاعتداءات الدوليّة، يتم اللجوء إلى المحكمة الجنائية الدوليّة أو محكمة العدل الدوليّة، أو مجلس الأمن من خلال الأمم المتحدة، أو الإنتربول، أمّا في حالات الإرهاب الالكتروني، أو الجريمة الإلكترونيّة أو الاعتداء السيبراني، كيف تتم المعالجة؟  
من هنا تقضي الضرورة وضع استراتيجية دوليّة للأمن السيبراني تعتمد على مبادىء متعددة أهمّها: وضع أسس التعاون الدولي، وضع تعليمات وإجراءات الوقاية والمعالجة، بناء القدرات البشريّة والتقنيّة المتطورة، وبالتالي تكون أدوات التنفيذ ضمن خيارات عدّة أهمها إنشاء محكمة سيبرانيّة دوليّة، إنشاء شرطة دوليّة سيبرانيّة، إنشاء قوة تدخّل سيبرانيّة باستخدام السلاح أو الوسائل الالكترونيّة المضادة، تفعيل التعاون الدولي، تفعيل التعاون بين القطاعين العام والخاص والمؤسسات الأمنيّة والشركات، إنشاء مراكز تدخّل ومعالجة وطنيّة، إجراء التشريعات والتعديلات اللازمة، والقيام بالإصلاحات التنظيميّة.  
على الرغم من الحاجة إلى اعتماد الاستراتيجية المذكورة، تبرز هناك بعض القيود المرتبطة بالسيادة الوطنيّة، الصراع بين الحريّة والأمن، نفوذ الدول العظمى، قرارات مجلس الأمن المرتبطة باستخدام حق النقد "Veto"، صعوبة إنجاز التعديلات القانونيّة والدستوريّة، هذا بالإضافة إلى بعض المعوقات، لا سيّما ما هو مرتبط بعدم وجود مرجعيّة دوليّة واحدة، عدم وجود خبرة تقنيّة كافية لدى القضاة والمحققين في هذا المجال، كيفيّة إدارة استخدام القوّة العسكريّة أو التقنيّة كردّ على بعض هذه الاعتداءات، من دون أن ننسى الحاجة إلى الدعم المادي المرتفع، إلّا أنّ المفكّر "بنجامين فرانكلين" يقول: "في حال فَشِلتَ في التخطيط، فإنك تخطط للفشل".