WHITE PAPER

# Cyberspace: the Fifth Domain of War!?

# Contents

**INTRODUCTION** ..... **3**
CYBER SPACE THE FIFTH DOMAIN OF WAR!? ..... 3
**UNDERSTANDING NATION-STATE STRATEGIES BEHIND ADVANCED CYBER ATTACKS** ..... **4**
NATION-STATE STRATEGIES ..... 4
CONFUSION OF WHAT IS A CYBER ATTACK AND CYBER WAR ..... 5
**OUTAGE OF NATIONAL CRITICAL INFRASTRUCTURE** ..... **6**
**CYBER DEFENCE OR CYBER WAR?** ..... **7**
OPERATION CLEAVER ..... 7
**NEW ACTORS AND NEW TECHNOLOGIES ON THE CYBER STAGE** ..... **8**
NEW ACTORS ON THE CYBER STAGE ..... 8
IRAN ..... 8
SYRIA ..... 9
NORTH KOREA ..... 9
INDIA AND PAKISTAN ..... 9
NEW TECHNOLOGIES ON THE CYBER STAGE - ISRAEL PRESENTS AN 'IRON DOME' FOR ENERGY SECTOR ..... 9
**GLOBAL CYBER GOVERNANCE FRAMEWORKS ARE INADEQUATE FOR HANDLING EMERGING TECHNOLOGIES.** ..... **10**
**CONCLUSION** ..... **11**
**REFERENCES** ..... **12**

## INTRODUCTION

While traditional information security has always included practice areas related to the security of information and systems, the cyber world that we live in today has become increasingly connected and increasingly mission critical due to our network-delivered society. The traditional enterprise boundaries that formed the basis for securing the perimeter from the outside world have, by necessity, become increasingly porous to support this new, routinely wireless and ubiquitous "always-on" connectivity.

The major challenge for organizations today is determining how to embrace disruptive technologies and trends such as "everything connected," cloud, mobile, and social computing, while at the same time managing the inherent risks that conducting business in cyberspace creates.

Before describing the cyber war motivations related to cyber security, it's important to understand the general definition and scope of the term and how it relates within the broader context of security. A useful definition comes from the UK's cyber security strategy:

"*Cyber Security embraces the protection of both private and public sector interest in cyber space and their dependency on digital networks and also the protection of exploitation of opportunities—commercial or public policy—that cyberspace offers.*"

While there are many definitions, the key point to note is that the scope of cyber security extends not only to the security of IT systems across the enterprise, but also to the broader digital networks upon which they rely, including cyberspace itself and critical infrastructures.

On a national level, many governments have deemed cyber security a tier one priority within their national security strategies, recognizing the likelihood and impact of potential attacks. One of the key implications of this definition of cyber security is that we now have a society dependent on network-delivered services.

Protecting this new dependency is what we call cyber security. It spans both the logical world of IT, i.e., bits and bytes and computers, as well as the "real world" of utilities, productions and services in cyberspace.

Everything we do is network-delivered, even crime. One of the imperatives for any cyber security strategy is therefore to take a more holistic approach to how we defend and protect our organizations, and even our society, and to help recover when things go wrong.

Security firm FireEye published in 2014 an interesting research titled "World War C" that describes the effort spent by governments in cyber warfare context, the document analyzes in detail the different approaches adopted by various countries in conducting nation-state driven cyber attacks.

## CYBER SPACE THE FIFTH DOMAIN OF WAR!?

*Cyberspace has become a full-blown war zone as governments across the globe clash for digital supremacy in a new, mostly invisible theater of operations. Once limited to opportunistic criminals, cyber attacks are becoming a key weapon for governments seeking to defend national sovereignty and project national power.*

From strategic cyber espionage campaigns, such as Moonlight Maze and Titan Rain, to the destructive, such as military cyber strikes on Ukraine, Georgia and Iran, human and international conflicts are entering a new phase in their long histories. In this shadowy battlefield, victories are fought with bits instead of bullets, malware instead of militias, and botnets instead of bombs.

These covert assaults are largely unseen by the public. Unlike the wars of yesteryear, this cyber war produces no dramatic images of exploding warheads, crumbled buildings, or fleeing civilians. But the list of casualties - which already includes some of the biggest names in technology, financial services, defense, government, steel industry and energy - is growing larger by the day.

A cyber attack is best understood not as an end in itself, but as a potentially powerful means to a wide variety of political, military, and economic goals.

Just as each country has a unique political system, history, and culture, state-sponsored attacks also have distinctive characteristics, which include everything from motivation to target to type of attack.

Cyber attacks have become both a concern for national security and a new tool in foreign policy.

Major cyber-incidents in the past few years have led to this assumption. In 2007, DDoS attacks against the Estonian government led to paralysis of public services in Estonia for three weeks, and marked the start of collaborative efforts to address the cyber warfare threat and to develop international norms for conduct in cyberspace. During the 2008 Russian–Georgian war, media and government websites in

Georgia came under attack from hackers. In 2010, the 'Stuxnet' computer worm, considered one of the most sophisticated cyber weapons to date and a possible first sight of cyber warfare, damaged uranium enrichment centrifuges at Iran's Natanz nuclear site. (Stuxnet has been compared to a 'cyber missile', aimed at destroying the physical infrastructure of Iran's nuclear plants).

And in 2012, a DDoS campaign against the US financial sector (Operation Ababil) was claimed by the group 'Izz ad-Din Al Qassam', but it is suspected that Iran was behind it , in retaliation for the Stuxnet attack. Although these incidents have not been attributed to particular states, suspicions persist that state actors sponsored them (besides Iran, Russia for the Estonian and Georgian cases, and the US and Israel with regard to the Stuxnet attack).

Recently, cyber attacks are said to have been used in the conflict in Ukraine, both by Russia and Ukraine, and also against NATO, whose websites were targeted by DDoS attacks in March 2014. In other conflicts in the Middle East, evidence points to cyber attacks being deployed in Israel, Syria and Iraq, again not clearly attributed to state sponsored actors (although, for example, involvement of Iranian and Turkish 'cyber forces' is alleged in the case of DDoS attacks against Israel).

The EU and some of its Member States have also been targets of cyber-attacks. Besides some economically driven cyber attacks (e.g. on the EU's carbon Emission Trading Scheme), others have been directed to the military: grounding French naval planes, securing access to the UK Ministry of Defence's classified networks or attacking the Estonian Ministry of Defence (2013).

Currently there is a 'black hole' over what constitutes an act of cyber war and what the appropriate response might be, a definition of what constitutes cyber warfare and whether it encompasses more than states as actors. For example, the US Department of Defense has defined cyber warfare as: ‘an armed conflict conducted in whole or in part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defence and cyber enabling actions.' The US goes on to define defensive and offensive capabilities, as well as the need for pre-emptive action in certain cases.

---

## Understanding Nation-State Strategies behind Advanced Cyber Attacks

---

“Iran should be considered a first-tier Cyber Power.”

**Gabi Siboni**

*Israel Institute for National Security Studies cyber security expert*

---

“Global Critical Infrastructure organizations need to take this threat seriously. The Iranian adversary is real and they’re coming, if not already here.”

**Mark Weatherford**

*Former Deputy Under Secretary for Cyber security at the US Department of Homeland Security*

---

“Yes, China and one or two others can Shut Down our Power Grids.”

**Admiral Michael Rogers**

*USA Director of the National Security Agency and head of USA Cyber Command*

---

### Nation-State Strategies

Here are some major strategic factors that will change the world’s Cyber Warfare:

1. **Outage of National Critical Infrastructure:** we know that cyber attacks can disrupt government or energy networks, but new cases of the last months are rising to the level of a national security threat. Stuxnet - and Iran’s alleged retaliation against the “West” in Operation Cleaver - has shifted the thinking

on cyber war from theory to reality. But have we seen the limit of what cyber attacks can achieve, or could cybercriminals threaten public safety by downing a power or telecom grid or financial market?

2. **Cyber Defence or Cyber War:** Cyber War is already upon us. if Nation-States and world leaders begin to view cyber attacks as a strategic weapon that can be used for offensive and defensive tasks, cyberspace will become the next battlefield. Snake malware has recently shown in the Ukraine the potential of espionage rootkits that are capable to destroy networks. 'Operation Cleaver' is showing Iran's capabilities in cyber attacks or cyber war? Several Defence organisation are creating Cyber Task Forces for defensive and offensive activities to protect or attack critical infrastructures.
3. **New Actors and New Technologies on the Cyber Stage:** the revolutionary nature of computers and the amplification power of networks are not exclusive to the world's largest nations. Iran, Syria, North Korea, and even non-state actors such as Anonymous have employed cyber attacks as a way to conduct diplomacy and wage war by other means. We see even so a stronger focus on evasion: some nation-states know how to launch stealthy cyber attacks. But as the discipline of cyber warfare matures, some "noisy" cyber attackers such as China may be forced to raise their game by trying to fly under a more finely tuned radar.

Cyber Attacks becomes one of the first weapons that Nation-States (sponsored groups) will activate to achieve their goals.

## Confusion of what is a Cyber Attack and Cyber War

There is a great confusion and uncertainty about what is Cyber War and what is a Cyber Attack.

- What is NOT Cyber War
  - A teenager defacing a DOD/MOD web site.
  - Criminals hacking into the bank accounts of a defence contractor to steal money.
  - An unfriendly nation stealing plans for a new jet fighter.
  - A terrorist group using the Internet for recruiting, fund raising, propaganda, and communications.
  - Countries stealing IP stored in computers from commercial firms.

*The dividing lines between criminal acts and acts that might implicate the UN charter of International Humanitarian Law (IHL) are unclear.*

- Cyber War is digital *conflicts* involving *politically* motivated attacks on information, information systems or critical infrastructures that has to be *potentially violent* and it has to be *purposeful*.
  - Cyber Warfare attacks can disable official websites and networks, disrupt or disable essential services in society or economy like energy and telecom, steal or alter classified data, and cripple financial systems - among many other possibilities.

So when we use the the term Cyber War it has to deal with the characteristics of politically motivated, potentially violent and to be purposeful.


The following examples of attacks could be illustrative of real Cyber War.

1. Operations conducted against Critical Infrastructures such as industrial control systems (so-called "SCADA" systems) to bring down the power or telecom networks, etc.
2. Cyber attacks on fundamental Internet protocols such as DNS (the domain name system) or BGP (the Internet's wide area routing protocols)
3. Kinetic ("physical") attacks on high value Internet "choke points" such as cable landing sites or Internet exchange points
4. Strategic high altitude strikes aimed at destroying or disrupting national infrastructure on a wide-scale through electromagnetic pulse (EMP) effects

## OUTAGE OF NATIONAL CRITICAL INFRASTRUCTURE

In the arsenal of government militias are entering strongly DDoS tools, spyware and computer viruses, nation-state driven cyber attacks are considerable an optimal option by governments for the following reasons:

- Reduced costs compared to conventional strikes.
- Efficiency
- The asymmetric nature of the cyber attacks makes difficult the defense.
- The anonymous nature of the offense allows the attacking government to circumvent the approval by the world community to a military offensive.
- Possibility to conduct cyber attacks in peacetime for immediate geopolitical ends, as well as to prepare for possible future kinetic attacks.

The attribution of responsibility for a cyber attack is a very hard task, FireEye experts correctly highlighted that to uncover the perpetrators is necessary to apply a multi layered approach based on forensic "reverse-hacking" techniques, build a deep knowledge of "patterns" of attack, evaluate the geopolitical context of cyber attacks aims associated to specific government.

*"A cyber attack, viewed outside of its geopolitical context, allows very little legal maneuvering room for the defending state," "False flag operations and the very nature of the internet makes tactical attribution a losing game. However, strategic attribution – fusing all sources of intelligence on a potential threat – allows a much higher level of confidence and more options for the decision maker," "And strategic attribution begins and ends with geopolitical analysis." said Professor Thomas Wingfield of the Marshall Centre, a joint US-German defense studies institute.*

*"The biggest challenge to deterring, defending against, or retaliating for cyber attacks is the problem of correctly identifying the perpetrator," said Prof. John Arquilla, Naval Postgraduate School.*

"Attribution" for a nation-state driven cyber attack is difficult due to similarity with methods adopted by single individuals, organizations, or state-sponsored hackers. States are often mistakenly identified as non-state entities, and vice versa. Another dangerous phenomenon that we are assisting is the growth of number of cyber mercenary groups close to governments that are structured as cyber criminal gangs but that are able to offer hacking services to involve in nation-state driven cyber attacks.

*"Cyber crime organizations offer anyone, including governments, cyber attack services to include denial-of-service attacks and access to previously compromised networks." states the World War C report.*

FireEye experts analyzed the Nation-state driven cyber attacks identifying the tactics and characteristics for the offensive in various regions:

- Asia-Pacific: home to large, bureaucratic hacker groups, such as the "Comment Crew" who pursues targets in high-frequency, brute-force attacks.
- Russia / Eastern Europe: More technically advanced cyber attacks that are often highly effective at evading detection.
- Middle East: Cybercriminals in the region often using creativity, deception, and social engineering to trick users into compromising their own computers.
- United States: origin of the most complex, targeted, and rigorously engineered cyber attack campaigns to date, such as the Stuxnet worm. Attackers favour a drone-like approach to malware delivery.

New players are entering the arena of cyber warfare strongly, countries such a North Korea, Iran and Syria have demonstrated to represent a serious menace also for the most industrialized super powers, this is the democracy of the new military doctrine. Examining most advanced countries in cyber warfare, China is considered responsible for the largest number of Nation-state driven cyber attacks, it uses high-volume noisly cyber attacks mainly for cyberespionage.

On the other end U.S.A., and Israel, providing the most advanced technologies, are able to conduct even so sophisticated and surgical cyber operations, Stuxnet and Duqu are just a couple of examples of products of joint effort spent by the two governments. The Russian Government is considered one of the entities with major cyber capabilities, like Israel and USA it is able to perform sophisticated nation-state driven cyber attacks, but little is known about the internal organization of its cyber units. According to rumors, a group of hackers that report directly to the President is the core of Russian cyber command that has operated in stealthily way in cyberspace against hostile governments and on the domestic front against opponents of the regime.

## CYBER DEFENCE OR CYBER WAR?

Cyber War is already upon us. Nation-state driven cyber attacks are routinely conducted on a global scale to defend national sovereignty and project national power. We are living in the cyber era, human conflict is involving also the fifth domain of warfare, the cyberspace. As never before disputes take place with blows of bits, militias of every government are developing cyber capabilities dedicating great effort for the establishment of cyber units.

"Cyber war is coming!" John Arquilla and David Ronfeldt predicted in a celebrated Rand paper back in 1993. William J. Lynn III, the deputy defense secretary in 2012, was writing that cyber war is "just as critical to military operations as land, sea, air, and space."

Time for a reality check: Cyber war is already upon us. Consider the definition of an act of war: It has to be potentially violent, it has to be purposeful, and it has to be political. The cyber attacks we've seen so far, from Estonia to the Stuxnet virus, simply don't meet these criteria but the massive cyber attacks from Iran in 'Operation Cleaver'is meeting these requirements.They are political driven, they are purposeful and they are potentially violent.

### OPERATION CLEAVER

Iran's 'Operation Cleaver' has, over the past several years, conducted a significant global surveillance and infiltration campaign. To date it has successfully *evaded detection* by existing security technologies. The group is believed to work from Tehran, Iran, although auxiliary team members were identified in other locations including the Netherlands, Canada, and the UK.

The group successfully leveraged both publicly available, and customized tools to attack and compromise targets around the globe. The targets include military, oil and gas, energy and utilities, transportation, airlines, airports, hospitals, telecommunications, technology, education, aerospace, Defense Industrial Base (DIB), chemical companies, and governments.

With minimal separation between private companies and the Iranian government, their modus operandi seems clear: blur the line between legitimate engineering companies and state sponsored cyber hacking teams to establish a foothold in the world's critical infrastructure.

Looking more in depth to what is reported about 'Operation Cleaver', security firm Cylance reports that what they discovered into this campaign represents only a fraction of Operation Cleaver's full scope. Cylance believes that if the operation is left to continue unabated, it is only a matter of time before the world's physical safety is impacted by it.

Iran's 'Operation Cleaver' is a combination of the examples 1 and 2 and within their interest the potention of 3 and 4.

Operation Cleaver Targets Critical Infrastructure around the World.

1. US Military targets including NMCI in October 2013. Confirmed targeting of global government entities.
2. Networks and systems targeted in critical industries like energy and utilities, oil and gas, and chemical companies.
3. Assets (both cyber and physical) and logistics information were compromised at major airline operators, airports, and transportation companies.
4. Various global telecommunications, technology, healthcare, aerospace, and defence companies were breached as part of the operation.
5. Confidential critical infrastructure documents were harvested from major educational institutions around the world.

Cylance is speculating about the motives behind Iran's cyber attacks based on the information they collected. This campaign continues Iran's retaliation for Stuxnet, Duqu, and Flame.

1. This is a state-sponsored campaign.
2. There is a possibility that this campaign could affect airline passenger safety.
3. This campaign's intentions may be to damage Industrial Control Systems (ICS), Supervisory
4. Control and Data Acquisition (SCADA) systems, and impact Critical Infrastructure and Key Resources (CIKR).
5. This campaign could be a way to demonstrate Iran's cyber capabilities for additional geopolitical leverage, due to the breadth and depth of their global targets.

6. There is an intense focus on CIKR companies in South Korea, which could give Iran additional clout in their burgeoning partnership with North Korea. In September 2012, Iran signed an extensive agreement for technology cooperation agreement with North Korea, which would allow for collaboration on various efforts including IT and security.
7. Iran is recruiting from within the universities and potentially using 'hackers for hire'.

Cylance discovered over 50 victims in their investigation, distributed around the globe. Ten of these victims are headquartered in the US and include a major airline, a medical university, an energy company specializing in natural gas production, an automobile manufacturer, a large defense contractor, and a major military installation. The four targets in Israel and the five targets in Pakistan are comprised of education, aerospace, airports, airlines, healthcare and technology. Further victims were identified in numerous Middle Eastern countries as well as ones in Northern Europe including the UK, France, and Germany. Central America was not immune either with a large oil and gas company on the list. In fact, oil and gas was a particular focal point for the Cleaver team, going after no less than nine of these companies around the world.

Universities were targeted in the US, India, Israel, and South Korea. The attackers targeted research efforts, student information, student housing, and financial aid systems. They had a penchant for pictures, passports, and any specific identifying information.

Perhaps the most bone-chilling evidence Cylance collected in this campaign was the targeting and compromise of transportation networks and systems such as airlines and airports in South Korea, Saudi Arabia and Pakistan. The level of access seemed ubiquitous: Active Directory domains were fully compromised, along with entire Cisco Edge switches, routers, and internal networking infrastructure. Fully compromised VPN credentials meant their entire remote access infrastructure and supply chain was under the control of the Cleaver team, allowing permanent persistence under compromised credentials. They achieved complete access to airport gates and their security control systems, potentially allowing them to spoof gate credentials.

What the report is showing is a shocking amount of access into the deepest parts of the attacked companies and the airports in which they operate. The Cleaver campaign used a variety of methods in multiple stages of attacks.

## New actors and New Technologies on the Cyber Stage

New players are entering the arena of cyber warfare strongly, countries such a North Korea, Iran and Syria have demonstrated to represent a serious menace also for the most industrialized super powers, this is the democracy of the new military doctrine. Examining most advanced countries in cyber warfare, China is considered responsible for the largest number of Nation-state driven cyber attacks, it uses high-volume noisily cyber attacks mainly for cyber espionage. However Iran should be considered a first-tier cyber power according to Gabi Siboni cyber security expert from the Israel Institute for National Security Studies. A last week (December 2014) published report of Security firm Cylance is reporting about what they called 'Operation Cleaver'.

### New Actors on the Cyber Stage

The revolutionary nature of computers and the amplification power of networks are not exclusive to the world's largest nations. Iran, Syria, North Korea, and even non-state actors such as Anonymous and IS with its Cyber Caliphate have employed cyber attacks as a way to conduct diplomacy and wage war by other means.

#### Iran

Iran's nation state sponsored Operation Cleaver has, over the past several years, conducted a significant global surveillance and infiltration campaign. To date it has successfully evaded detection by existing security technologies. The group is believed to work from Tehran, Iran, although auxiliary team members were identified in other locations including the Netherlands, Canada, and the UK.

The group successfully leveraged both publicly available, and customized tools to attack and compromise targets around the globe. The targets include military, oil and gas, energy and utilities, transportation, airlines, airports, hospitals, telecommunications, technology, education, aerospace, Defense Industrial Base (DIB), chemical companies, and governments.

With minimal separation between private companies and the Iranian government, their modus operandi seems clear: blur the line between legitimate engineering companies and state sponsored cyber hacking teams to establish a foothold in the world's critical infrastructure.

### SYRIA

The Syrian Electronic Army (SEA) is a group of computer hackers who support the government of Syrian President Bashar al-Assad. Using spamming, defacement, malware (including the Blackworm tool), phishing, and denial of service attacks, it mainly targets political opposition groups and western websites including news organizations and human rights groups. The Syrian Electronic Army is the first public, virtual army in the Arab world to openly launch cyber attacks on its opponents.

The precise nature of its relationship with the Syrian government is unclear. The SEA claims to be "a group of enthusiastic Syrian youths who could not stay passive towards the massive distortion of facts about the recent uprising in Syria", though several experts believe the group is supervised by the Syrian state.

### NORTH KOREA

Due to ongoing regional and global tensions, everything that North Korea does is of interest to national security thinkers around the world, especially when it involves asymmetric capabilities such as weapons of mass destruction (WMD) and computer hacking.

North Korea launched its first cyber attack on U.S. and South Korean government websites in 2009. There was little damage done, but the incident gained wide media exposure. By 2013, North Korean hackers had matured. A group called the “DarkSeoul Gang” is believed to be responsible for high-profile operations against South Korea over a period of at least four years, including DDoS attacks and the insertion of malicious code that wiped computer hard drives at banks, media outlets, ISPs, and telecommunications and financial firms, overwriting legitimate data with political messages. Suspected North Korean attacks on U.S. targets include military units based in South Korea, the U.S.-based Committee for Human Rights in North Korea, and the White House. Such incidents often take place on dates of historical significance, including July 4th, the U.S. Independence Day.

North Korean defectors have described a burgeoning cyber warfare department of 3,000 personnel, likely trained in China or Russia. They believe that North Korea has a growing “fascination” with cyber attacks as a cost-effective way to target conventionally superior foes, and that North Korea is growing increasingly comfortable and confident in this new warfare domain, assessing at least two things: that the internet is vulnerable, and that cyber attacks can put psychological pressure on the West. To this end, North Korea has ensured that its own national servers are not connected to the internet, while simultaneously building a dedicated “attack network”.

As with China, North Korea asserts that it too is a victim of cyber attacks. In June 2013, when the North suffered a two-day outage of all of its in-country websites, North Korean reporters denounced “concentrated and persistent virus attacks” and proclaimed that the U.S. and South Korea “will have to take the responsibility for the whole consequences.” Pyongyang also noted that the attack took place coincident with Key Resolve, a joint U.S.-South Korean military exercise. The South Korean Joint Chiefs of Staff denied any connection.

### INDIA AND PAKISTAN

As a final example, it is important to remember that wherever there is historical tension in the “real world”, there is now parallel tension in cyberspace. Although a heavily fortified border separates India and Pakistan on a traditional map, the quiet, borderless nature of the internet means that both sides are free to engage in computer hacking, even during peacetime.

In 2009, India announced that Pakistani hackers had placed malware on popular Indian music download sites as a clever and indirect way to compromise Indian systems. In 2010, the “Pakistani Cyber Army” defaced and subsequently shut down the website of the Central Bureau of Investigation, India's top police agency. In 2012, over one hundred Indian government websites were compromised. India, for its part, appears responsible for “Operation Hangover”, a large-scale cyber espionage campaign in which Pakistani information technology, mining, automotive, legal, engineering, food service, military, and financial networks were targeted.

## NEW TECHNOLOGIES ON THE CYBER STAGE - ISRAEL PRESENTS AN ‘IRON DOME’ FOR ENERGY SECTOR

The Israel Electric Company (IEC) is concerned about protection of the Jewish nation’s electrical grid. The recent 50 day summer 2014 war with Hamas in Gaza witnessed more than 2,300 rockets reining death and destruction on Central and Southern Israel. Several hundred rockets headed towards major population centers in the State of Israel were detected and literally knocked from the skies by the Iron Dome system batteries. Hamas and Palestinian Islamic Jihad rockets over the period from 2006 to 2014 have targeted the Rutenberg Power Plant of the IEC in Ashkelon. The power plant has also been subject to periodic outages. The vulnerability to physical attack was illustrated by Gaza’s sole power plant destroyed during the conflict.

# Israel presents an 'Iron Dome' for 'electricity terror'

Company that pioneered technology to stop rockets has developed a way to keep terrorists from attacking the country's grid

BY DAVID SHAMAH | November 11, 2014, 7:44 pm | 9

Physical threats are only one aspect. There are also Electromagnetic Pulse (EMP) and cyber attacks. Cyber attacks on critical operating systems, such as Siemens' SCADA (Supervisory Control and Data Acquisition) are something that Israel may know about. There was the development of the Stuxnet malware that disrupted Iran's nuclear enrichment program. Israel to this day remains silent about any involvement in the malware's development. Israel's electrical network vulnerabilities led the IEC to partner with the Israeli firm of mPrest that had developed the critical sensor and detection software system at the core of the Iron Dome System. The objective was to develop a means of intercepting and deterring cyber threats to the national grid. The Information Grid (IG) system was unveiled at a Homeland Security Conference in Tel Aviv.

But if Stuxnet was unique and exceptional just two years ago, it's just another run-of-the-mill attack program now. Over the past several years, there's been an explosion in the development of malware to attack infrastructure, SCADA systems, the automated low-level computer systems that control machinery, transportation systems, gas stations, utility systems, security installations – and electrical grids.

There is an international army consisting of tens of thousands of engineers out there developing SCADA malware. One day, a terrorist organization is going to get the bright idea to acquire one of these tools and deploy it to make their ideological point. If it hasn't happened yet, it's just a matter of time until it does.

Hoping to avoid a situation in which Israelis are victims of an "ideological point" made by Hamas or another terrorist group, the IEC partnered with a subsidiary of mPrest Systems, called mPrest Electric, which was a member of the IEC's KARAT Incubator. Drawing on the tech used by mPrest to design and operate Iron Dome, the companies designed the Information Grid, which checks the flow of electricity to ensure that lines are not overloaded, and that electricity "viruses" — attacks on specific sections of the grid – don't spread, allowing administrators to quickly identify suspicious activity and isolate it.

As with Iron Dome, the key to the Grid's capabilities is the creation of specific rules that quickly deploy resources and issue commands on the grid in response to ever-changing circumstances. The heart of the Grid is a command and control system similar to the one that controls Iron Dome. When an attack is detected – if a SCADA system that is controlling electrical flow starts acting "funny," for example – the Grid will notice it right away, and it will automatically shut off connections to the substation or segment of the system that has been compromised, preventing further damage and allowing security personnel to better track the source of the attack.

The system allows integration and control in real-time of thousands of sensors, which are installed at about 300 different sites in Israel. The sensors measure a wide variety of data, which flows into the Grid and is analyzed in real time. The Grid is based on a unique architecture which allows the integration of an infinite number of systems and assets, with no limitation on the number of links or data, said the IEC, and it can also handle additional information from a wide variety of legacy programs that measure and record data.

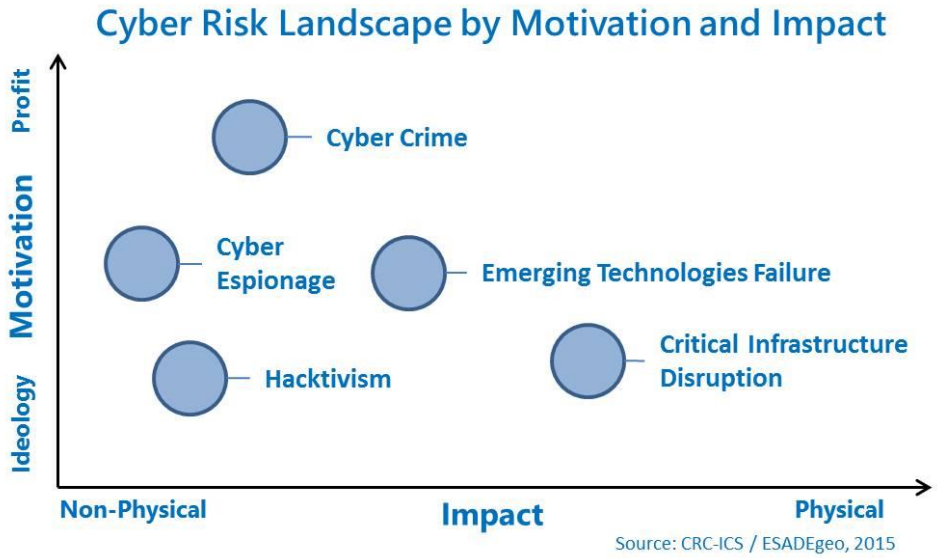
To ensure full preparedness, the Grid prepares potential problem scenarios based on permutations of the data, providing daily "what if" scenarios and solutions based on the trends it discovers in the electrical system.

According to the chairman of the board of directors of the Israel Electric Company, "Hezbollah-style terrorism and Grad missile attacks are out; cyber-attacks are in. We are getting hit with tens of thousands of penetration attempts daily, hundreds of thousands monthly. The world, the state of Israel and the electricity sector are in an era where cybernetic threats on communication infrastructures are ever increasing. I attach great importance to training future generations. As chairman of the board of the IEC, I can testify to the abilities we are developing in the field of cybernetics which places us in the forefront of this sophisticated and complex arena."

## GLOBAL CYBER GOVERNANCE FRAMEWORKS ARE INADEQUATE FOR HANDLING EMERGING TECHNOLOGIES.

The current state of regulation and the governance regimes in place globally are inadequate to ensure the security of the world's cyber infrastructure, argues a 2015 Zurich Insurance Group and ESADE Center for Global Economy and Geopolitics report. The report – which examines both the current and evolving nature of cyber risk and the existing global governance framework, as well as proposes new paths to tackle the current

disorder in cyber space – points to inadequate preparation to handle new technologies, including drones, 3-D printing and self-driving cars. Newly emerging technologies will impact the security of the Internet, it concludes.




Zurich reports in the statement that companies in almost all sectors are exposed to cyber threats, with the potential for causing enormous damage in terms of reputation and physical losses, liabilities and regulatory costs. “Unchecked, growing cyber threats risk curtailing technical and economic development on a global scale,” the statement adds.

The existing governance framework from the 20th century cannot be expected to respond sufficiently to a 21st century technology.“We live in a world full of opportunities, but also risks. The cyber realm underpins almost all economic and societal activity – from finance to trade, information, energy and beyond.

In the event of a global cyber shock, it is not clear who would be in charge and what levers could be used to reduce the impact on the internet and society. The report also states that geopolitical and ideological tensions between states are increasingly played out in cyber space, including over matters of governance.

The nature of cyber security is evolving so quickly it can be difficult for businesses to keep track of the risks let alone the solutions. It is very clear that businesses that want to protect themselves from security, cyber security and privacy risks must adopt a mindset of resilience.

“The world needs a fluid and more comprehensive dialogue between business, politics and civil society to ensure the security of cyberspace. Developing an inclusive and reliable governance regime for the security of the cyber realm is a prerequisite to managing the risks and grasping the opportunities that emerging technology presents.

Recommendations to policymakers include creating a G20 + 20 Cyber Stability Board, made up of the 20 largest governments and the 20 largest tech firms, for strengthening global institutions and taking steps to isolate these institutions from geopolitical tensions; and creating a Cyber WHO (World Health Organization) to enhance crisis management, the Zurich report adds.

In addition, the private sector must engage in sharing information and employ an approach that will increase their overall cyber resilience to address the inadequacies of the framework, the statement adds.

Whatever public-private cyber security regimes or collective actions may develop, it is incumbent on businesses to take a pragmatic approach to the cyber governance gap that is likely to persist for the next few years, the report suggests. This includes investment in studying and enhancing protection against cyber risks, as well as creating a culture of cyber resilience.

## CONCLUSION

Nations today use computer network operations to defend sovereignty and to project power, and cyber conflicts is today the rule rather than the exception. Most cyber attacks do not rise to the level of a national security threat, but in the post-Stuxnet era, the notion of “cyber war” has moved to reality.

There is often a strong correlation between the sophistication of a cyber attack and its geopolitical context. In the case of Iran, the question at hand was whether to allow a new nation into the world's nuclear club; it was one of the most important questions that international security decision makers could face. Therefore, it is not surprising that Stuxnet, the malware discovered inside the Iranian nuclear program, was the most advanced malicious code that public researchers have seen.

In the near future, the size of the international cyber stage and the number of actors upon it will grow. Governments will both want and need to flex their digital muscles in order to gain a comparative advantage in political and military affairs as well as to create some level of cyber attack deterrence.

For all nations, an important consideration is the risk of cyber counterattack. The Aramco reprisal, for example, showed that all modern economies are dependent on information technology, and that worldwide connectivity, coupled with the prevalence of cyber vulnerabilities, cuts both ways. Remember that Iraqi insurgents used $26 off-the-shelf software to intercept live video feeds from U.S. Predator drones. There have yet to be any major outages of public critical infrastructure due to cyber attack, but for world leaders, that could be a game changer. One day, we may have a cyber arms control regime or an international non-aggression pact for cyberspace. However, the difficulty of defining malicious code, as well as the challenge of inspecting for it, would make that easier said than done.

Some governments have already begun to take political action to shore up the technical deficiencies in their cyber defences. In 2013, President Obama directed that the U.S. would aid allies who come under foreign cyber attack, and the U.S. and Russia signed an agreement to build a cyber "hotline" similar to that used for nuclear scares during the Cold War. Fundamentally, an international problem like cyber security will require an international solution, and the European Union and NATO, as the largest and most cohesive political and military alliances in the world, are the best places to start.

## REFERENCES


- Cisco, "Annual Security Report", 2014.
- Cylance Report – Operation Cleaver; December 2014.
- FireEye Report – World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks; January 2014.
- Israel National News - http://www.israelnationalnews.com/Blogs/Message.aspx/6469 ;September 2014
- Symantec Report - Regin: Top-tier espionage tool enables stealthy surveillance; November 2014.
- Symantec Report – Dragonfly: Cyberespionage Attacks Against Energy Suppliers; July 2014.
- Tallin Papers - Pandemonium: Nation-States, National Security and the Internet; 2014.
- USA National Research Council; "Technology, Policy, Law and Ethics Regarding U.S. Acquisitions and use of Cyber Capabilities", 2009.
- USA NIST, "Cyber Security Framework for Critical Infrastructures"; 2014.
- EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL; October 2014.
- Zurich Insurance Group and ESADE Center for Global Economy and Geopolitics, report; April 2015.