CERI STRATEGY PAPERS
N° 7 – Rencontre Stratégique du 30 avril 2010

Cyber Vs. Nuclear

Boaz DOLEV and Assaf KEREN

Boaz Dolev is Director of eVision Systems Ltd. Assaf Keren is Vice-President, Methodology and Strategy at CyberVision Security Solutions. Both authors are former leaders of IT Security at the Israeli E-Gov Division.

"A war of pure coercion where each side restrained by the apprehension of the other's response. It is a war of pure pain; neither gain for the pain it inflicts, but inflicts it to show more pain can come. It would be a war of punishment, of demonstration, of threat, of dare and challenge. Resolution, bravery, and genuine obstinacy would not necessarily win the contest. An enemy's belief in one's obstinacy might persuade him to quit. But since recognized obstinacy would be an advantage, displays or pretenses of obstinacy would be suspect. We are talking about a bargaining process, and no mathematical equation will predict the outcome."
Thomas Schelling, *Nuclear War*, 1966, p. 201,

Introduction

In the past five years, the use of cyber attacks and cyber weapons has become one of the main concerns for governments and organizations alike. Whether the attacks have been aimed at shutting down entire countries or stealing sensitive information, both state and private organizations have been faced with the need to handle this emerging threat. Several state and government organizations around the world have stated that the threat of cyber attacks against their countries' is equivalent to the threat or use of weapons of mass[12] destruction, specifically the use of nuclear arms.

This article will review and compare the main attributes of these weapons, nuclear and cyber, and will attempt to determine a similarity between these weapons.

When examining these weapons, we have identified four categories:
- Country or user attributes;
- Weapon attributes;
- Primary and secondary weapon effects;
- International treaties and supervision.

Unique examples, nuances and expertise are associated with each category. Consequently, we chose to focus on the main attributes in each category in order to capture a larger view on both worlds.

---

[1] http://www.siliconvalleywatcher.com/mt/archives/2010/02/former_us_intel.php
[2] http://gsn.nti.org/gsn/nw_20090512_4977.php

Cyber attack definition

Cyber attack is the deliberate disruption or corruption by one state of a system of interest to another state. The former state will be referred to as the "Attacker"; the latter state will be referred to as the "Target". In some contexts, the target may also become a "Retaliator". The affected system will be referred to as the Target System (cf. *Cyber Deterrence and Cyber War*, Martin C. Libicki).

Threat analysis

In our effort to understand the threat against countries and private organizations we must divide the threat landscape into the different types of attackers that we face.

Hackers / computer enthusiasts
In the overall scope of threat hackers and computer enthusiasts are the lowest level of attackers. These individuals usually have no political agenda and are motivated by fame or intrigue. Most of the individual attackers will stop prior to conducting actual damage to systems and will usually notify the attacked organizations about flaws in their systems.

Hacktivism
Hacktivism groups are more sophisticated and more organized than individual hackers. These groups have some kind of political agenda, and have decided to campaign for their agenda online, either by defacing websites, shutting down systems or just sending spam to specific targets. Hacktivism has been practiced online for a long time having started during the days of ARPANET.

Terror organizations
Terror organizations started using the web when they found it to be a safe tool for sending and receiving messages and using the anonymity of the web as a means of promoting their agenda. Only years later did they start to use the web as a means to raise funds and now are working to create cyber weapons.

Criminal organizations
Criminal organizations are some of the stronger players in the cyber world today. In the last four years criminal organizations have started using the web for a steady stream of revenue. Stolen credit cards, bank accounts, identification factors, etc. are sold freely on the Internet today, making the web a very lucrative and interesting target for organized crime. Organized crime is in charge of more than 90% of the spam messages in the world and 80% of the malicious code being written today (for purposes other than research). It has established itself as a force on the Internet. It has been suggested that in some cases, it has served as a proxy for countries seeking to deny involvement in attacks. (Russian Business Network in the cyber attacks against Estonia and Georgia).

State operations

It has been rumored that state operations in cyberspace have been going on since the establishment of the Internet, although in the last few years we have been seeing a growing presence of allegedly state-funded operations in cyberspace. Whether the attacker has a political agenda (Estonia and Georgia), is an intelligence-gathering effort (Ghostnet, Aurora) or an attack on critical infrastructure (Stuxnet) it appears that more and more countries have taken to cyberspace in order to gain the upper hand against their enemies.

Timeline of significant events[1]

2003-2005: Titan Rain

Titan Rain was the U.S. government's designation given to a series of coordinated attacks on American computer systems since 2003. The attacks were labeled as Chinese in origin, although their precise nature (i.e., state-sponsored espionage, corporate espionage, or random hacker attacks) and their real identities (i.e., masked by proxy, zombie computer, spyware/virus infected) remain unknown.

2007: Estonia

The cyber attacks on Estonia refers to a series of cyber attacks that began April 27, 2007 and swamped websites of Estonian organizations, including the Estonian parliament, banks, ministries, newspapers and broadcasters. The attacks occurred during the country's dispute with Russia over the relocation of the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn. Most of the attacks that affected the general public were denial of service type attacks ranging from single individuals using various low-tech methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements, including that of the Estonian Reform Party website, also occurred.

2007: Oak Ridge National Laboratory

During 2007, alleged Chinese hackers penetrated two US nuclear research laboratories, ORNL being the more prominent of the two. It was reported that social security numbers, names and dates of scientists visiting Oak Ridge were stolen by the hackers.

2008: Lithuania

After Lithuania enacted a law banning the use of Soviet era symbols in demonstrations, attacks focused on website defacements began. These attacks resembled those in Estonia but were less strong in volume and intensity.

[1] All event descriptions were taken from Wikipedia (www.wikipedia.org)

2008: Georgia
During the 2008 South Ossetia war a series of cyber-attacks swamped and disabled websites of numerous South Ossetia, Russian, Georgian, and Azerbaijani organizations.

2009: Ghost-net
Ghost-Net is the name given by researchers at the Information Warfare Monitor to a large-scale cyber spying operation discovered in March 2009. Its command and control infrastructure is based mainly in the People's Republic of China and has infiltrated high-value political, economic and media locations in 103 countries. Computer systems belonging to embassies, foreign ministries and other government offices, and the Dalai Lama's Tibetan exile centers in India, London and New York City were compromised. Although the activity is mostly based in China there is no conclusive evidence that the Chinese government is involved in its operation.

2009: Operation Aurora
Operation Aurora is a cyber attack, which began in mid-2009 and continued through December 2009. The attack was first publicly disclosed by Google on January 12, 2010.
The attack was aimed at dozens of other organizations. Adobe Systems, Juniper Networks and Rackspace have publicly confirmed that they were targeted. According to media reports, Yahoo, Symantec, Northrop Grumman and Dow Chemical were also among the targets.
As a result of the attack, Google stated in its blog that it plans to operate a completely uncensored version of its search engine in China "within the law, if at all", and acknowledged that if this is not possible it may leave China and close its Chinese offices. In the blog post, Google said the attack originated in China.

2010: Stuxnet
Stuxnet is a Windows-specific computer worm first discovered in June 2010 by VirusBlokAda, a security firm based in Belarus. It is the first discovered worm that spies on and reprograms industrial systems. It was specifically written to attack Supervisory Control and Data Acquisition (SCADA) systems used to control and monitor industrial processes. Stuxnet includes the capability to reprogram the programmable logic controllers (PLCs) and hide the changes.

Country or user attributes

The attributes relating to countries or users of the specific weapons:

Manufacturing abilities
The creation of nuclear weapons is probably the most highly regarded technological frontier in the history of mankind.

Starting from inception would take a state approximately 10 years to create a functioning atomic bomb. With additional help and optimized conditions it can be reduced to several years. But the technological process is long, and requires expertise to achieve the most basic of nuclear weapons. In order to produce nuclear weapons an organization would need to build research facilities, production facilities and nuclear reactors. At some point the organization would need to apply and implement safety and security procedures, and invest in peripheral personnel and logistics aspects, not directly connected to basic nuclear research.
Another step in the creation of nuclear weapons is the testing phase. In order to qualify as a weapon the device must be reliable. Nuclear testing is highly detectable, if a nation wants to conduct "undetectable" nuclear testing extreme steps must be taken, and there will still be great risk of exposure to intelligence gathering organizations.
However, cyber weapons are not a big technological challenge. In order to build a cyber weapon an organization or a state only requires *qualified* computer science experts, not necessarily academics (arguably, non-academics have more experience in the cyber security field). The entire facility to create cyber weapons requires computers, servers and an Internet connection. Here we come to a discussion about the nature of cyber weapons as opposed to *Malicious Code*. However, it has been widely acknowledged that states can and will use commercial botnets and other malicious code, which makes the next cyber weapon author a much more ubiquitous organism. Any amateur that can buy or build a "Zeus Trojan" can potentially become the next cyber weapon creator. In conclusion, there are no means or infrastructure to supervise or control manufacturing of cyber weapons. Stakeholders opposed to nuclear weapons include not only countries but also "Non-State" organizations and criminal elements.

Ability to maintain

The maintenance of nuclear weapons is the next hurdle for a country aspiring to join the nuclear-club. Protocols and procedures needed to ensure safety, functionality and proper use of the weapons can fill books[1]. The ability to maintain nuclear weapons depends on having physical infrastructure. In order to create required storage facilities for nuclear arms the state most be able to handle delivery systems (such as missile, submarine, airplane).It must also be able to handle by-products of the core creation process (nuclear waste) and have storage facilities and safety mechanisms to support the nuclear weapons themselves. In contrast cyber weaponry requires no physical framework besides normal IT infrastructure. However, nuclear weapons are designed and produced to last decades. The ability of a nuclear weapon to create damage is never ending. In contrast, a cyber-weapon that relies on a specific vulnerability can be thwarted with a single patch.

Second strike capability or creating an equivalent strike deterrent

In the context of the global race to acquire nuclear weapons, the question arises as to how can to deter a state from a surprise nuclear strike that will “wipe out”

[1] Nuclear Weapons Maintenance Procedures - http://www.fas.org/irp/doddir/usaf/afi21-204.pdf

the enemy in a number of minutes. The solution is to counter attack the attacking state even after a nuclear strike in order to deter a second nuclear attack. To create second strike capability, nuclear submarines are deployed at all times and launching bases are established in other regions.

This results in a “balanced deterrent” which has prevented the use of nuclear weapons for decades. In the case of cyber weapons, on the other hand, significant gaps are immediately revealed. Following a cyber attack it is unclear whether a state can launch a “counter cyber attack”. Because a state can prepare for cyber attacks, timely and immediate reactions can thwart further attacks. For example, increased monitoring of computer systems, disabling non-essential systems, blocking the state network from the internet and further actions prepare the state for counter attacks. Theoretically, repetitive strike capabilities must be examined as no real “equivalent strike deterrent” currently exists in the cyber world and it is unclear if it is possible to create this type of deterrent. The result is that it is easier for a state to pull the cyber trigger than the nuclear trigger.

Technological maturity

Strategic weapons at different stages of technological maturity exist globally, as nuclear weapon production systems have been operating for decades in many countries. The establishment of nuclear weapon production systems and /or operations requires diverse technological expertise in areas such as physics, mathematics, nuclear science, computers, engineering, aeronautics, construction, and electricity. Nuclear weaponry is identified as having reached a technical maturity and is recognized as the ultimate threat deterrent.

“Cyber weapons” have been produced in a number of organizations and countries in recent years (5 years). The only experts necessary for the production of “cyber weapons” are computer experts, including hackers with no formal education. It is possible, although in our opinion unlikely, that in coming years through technological advances a means will be found to limit the ability to perform cyber attacks.

Budgetary constraints

One of the crucial questions when comparing cyber solutions is cost. The calculation should include design and production costs as well as long-term operating costs and, if possible, quantify the financial benefits behind the establishment of the project.

Establishing and operating nuclear weapon production plants requires a cumulative investment of tens of billions of dollars. The current “production” operating budget is dependent on the size, capacity, launch platform and storage infrastructure which can account for hundreds of millions of dollars and result in an ultimate investment of billions of dollars.

The costs incurred with establishing and maintaining “cyber weapons” varies depending on scale, production capability and accompanying research and development. Costs range from an insignificant initial investments, as low as hundreds of thousands of dollars annually to as high billions of dollars. Currently no real budgetary constraints exist to enter the cyber weaponry world.

Weapon attributes

In this section we will discuss attributes relating to the weapons themselves.

Previous use and consequences

Nuclear weapons have been used twice in modern history[1] by US forces on Hiroshima and Nagasaki, resulting in up to 200,000 casualties. These events are burned into our memory as two major historical events. Fear of the proven consequences of the use of nuclear weapons triggered the period of the cold war, without addressing the effect on the Japanese or the American world view.

In examining the history of Cyber weapons two incidents are key: Estonia and Georgia.

The Estonian case of 2007 is widely regarded at the first cyber war[2][3]. However, when we take a closer look at this event, based on a review by NATO's CCDCOE, we conclude that no country was held accountable for the attacks on the Estonian Internet Infrastructure. We also found that no fatalities resulted from the attacks and that only minor damage was reported on Internet sites. Equally, they had little importance to the Estonian Government as they caused only minor financial and political effects. The same can be said for the Georgian case in 2008. Both of the attacks came at a time of political tension, one during a clear state of warfare between Russia and Georgia. Nevertheless, it can be argued that the most damage caused by cyber weapons was in the field of cyber intelligence and not cyber warfare.

Indicators

One of the more interesting comparisons between nuclear and cyber weapons involves the use of indicators to reveal their availability There are many indicators of the development of nuclear weapons, such as:

- Creation of the weapons manufacturing plant (Reactor)
- Procurement of technologies related to weapons manufacturing (Centrifuges)
- Procurement of material and equipment specific for nuclear weapon development.
- Establishment of nuclear storage facilities.
- Weapons testing.
- Establishment of a proper delivery and launch system capabilities.
- Recruitment of scientists and researchers in the fields of expertise needed for nuclear weapons development.
- Large budgetary investment, difficult to camouflage in the overall state budget.

In the case of cyber weapons there are only indirect indicators of a state's capabilities. These include:

[1] http://en.wikipedia.org/wiki/Atomic_bombings_of_Hiroshima_and_Nagasaki
[2] http://www.guardian.co.uk/world/2007/may/17/topstories3.russia
[3] http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1

- The ability to deploy a cyber-weapon might be a derivative of the overall capability of the state and its armed forces in the Information Technology field.
- The amount of cyber crime / hacktivism / hacking attempts done by people belonging to the state, including organizations which are identified as belonging to a specific state.
- Prior attacks by state or attacks suspected to have emanated by the state.
- The amount of "political" talk about cyber weapons in conventions or by politicians.

It is easy for a state to camouflage development of cyber weapons. Consequently, a state that wishes to "stay off the radar" can develop such weaponry with a small team of experts and basic computing hardware. The ability to "outsource" cyber weaponry as well as new capabilities in the field has led to the production of "off the shelf" products.

Use-case scenarios

When examining nuclear weapons, we can see 5 different use cases. They are, by level of severity: deterrence, EMP[1], second strike, first strike, and all-out attack. Excluding deterrence, all levels have severe implications and damage on the attacked country. Whereas cyber weapons can be used in a wide variety of ways from web defacement and propaganda means, intelligence, critical infrastructure attacks, attack on government stability as well as deterrence from conventional and nuclear attacks.

Control of payload and effect

The capability of nuclear weapons to do physical damage is well defined and is determined by the characteristics of the nuclear package in the payload (and is measured accurately by kilotons and megatons). The effect of nuclear weapons is determined both by the payload and the environmental conditions at the target. This means the effect is not 100% clear, however it is, to a certain degree, controllable. Cyber weapons, in contrast, are usually aimed at specific targets but, considering the ambiguity of the ICT world, also can be used to attack a wider range of targets. Another possibility is that the defense systems may be sufficiently effective that no damage will be inflicted upon the attacked organization. Thus, in order to create a successful attack on a specific target and on a specific date, a country will need to have a sustainable presence in the attacked target.

Source signature (attribution)

Attribution is probably the single most important factor difference between cyber weapons and nuclear weapons. As formerly discussed in indicators *(See section 3.1)*, the traceability of nuclear weapons depends upon the availability of nuclear weapons in a specific country. However, when we discuss the actual usage of nuclear weapons, the delivery systems are usually massive (rockets, missiles, aircraft, submarines), and the determination of the source of the attack is usually straightforward. However, in the case of cyber technologies proxies, hacked

[1] http://en.wikipedia.org/wiki/Electromagnetic_pulse

machines and routing and rerouting of traffic make it easy for the attacker not only to hide his/her own origin but also to make it seem another country is the source of the attack. Misrepresenting not only the geographical origin but also the political motivation. While nuclear weapons are available only to countries, cyber weapons can be (and have been) used by criminals, anarchists, hackers and others. Consequently, when a cyber attack originates from a state it is not always clear whether the attackers are state-funded and -operated or simply a group of hackers who may or may not be supported by the state. [1]

Primary and secondary effects of the weapon

In this section we will discuss attributes relating to the actual effects of the weapons.

Damage capability

The damage capability of a nuclear weapon is straightforward (and was discussed in the previous section). In addition to dirty bombs, nuclear devices cause physical damage and, on occasion, electronic damage as well. The effects of the nuclear device do not go beyond the known damage aspects and are also limited to a geographical location. Cyber weapons can create other effects altogether, including loss and corruption of data, disinformation and denial of service as well as physical damage. The geographical aspect is also a non-issue in the cyber world; basically a cyber attacker can attack an entire country in a single attack.

Long-term effects

The long-term effect of nuclear weapons is recognized as being radiation effects. Long-term effects of cyber weapons depend on the specifics of the actual attack . For instance, an attack on a government website is very short-lived whereas an attack on an electrical grid or a water dam can have long-term effects.

Unintended consequences and cascading effects

Both nuclear and cyber worlds contain unintended consequences and cascading effects that were not included in the initial attack plan. In both these realms, the consequences are the outcome of poor planning and/or lack of proper intelligence. However, the numbers of factors that can create unintended consequences in the nuclear world are limited and can probably be dealt with in advance. In the cyber world, there are untold factors that can create undesired effects, and as a result it is harder to anticipate and plan for unintended consequences and cascading effects.

Stealth capability

Basically, the detonation of a nuclear device results in physical evidence: death, devastated buildings and sometimes even a hole in the ground. A state cannot stealthily attack another state. However, cyber weapons can be used stealthily,

---

[1] http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

and if the attacking side is sufficiently competent, the attack may even go completely unnoticed by the attacked country.

International treaties and supervision

In this section we will discuss the international control mechanisms over the weapons.

International cooperation to prevent usage

In the international arena, nuclear weapons have been discussed and legalized since World War II. International bodies have been established to control the development of nuclear technology[1] Including the General Assembly First Committee[2] and the International Atomic Energy Agency[3]. The development of nuclear weapons is frowned upon internationally. Developers may be sanctioned[4] or even becoming an international exile. Cyber weaponry largely is overlooked, as few multilateral treaties have been signed in this field. The most notable are the Council of Europe Convention on Cybercrime[5] and the Shanghai Cooperation Organization Statement on International Information Security. Neither of these calls for international cooperation.

Proliferation

While nuclear nonproliferation seems a feasible goal with the help of the NNPT[6] and the fact that nuclear technology can be defined and controlled. This is not the case with cyber weapons proliferation because it can be accomplished with a single click such as an e-mail message or a transfer of a disk-on-key between two people.

Protective umbrella

A nuclear umbrella[7] is a viable option for members of the nuclear club and their allies, sometimes even as a means to prevent further development of nuclear weapons by non-nuclear states. It is not impossible that a cyber umbrella will emerge in the future. One instance where this might have occurred were the discussions regarding the invocation of NATO's article 5[8] during the Estonia crisis of 2007. However, the Estonian case illustrates the true problem – attribution. It does not seem likely that a state would act violently (in the physical or the cyber world) if the attacker's identity was not known with certainty.

Supervision ability

Supervision capabilities for nuclear weapons are constantly being developed by the international bodies responsible for non-proliferation and disarmament.

[1] http://en.wikipedia.org/wiki/Nuclear_weapons#Governance.2C_control.2C_and_law
[2] http://en.wikipedia.org/wiki/General_Assembly_First_Committee
[3] http://en.wikipedia.org/wiki/International_Atomic_Energy_Agency
[4] http://en.wikipedia.org/wiki/Iran_nuclear_program#2007.E2.80.93present
[5] http://en.wikipedia.org/wiki/Council_of_Europe_Convention_on_Cybercrime
[6] http://en.wikipedia.org/wiki/Nuclear_Non-Proliferation_Treaty
[7] http://en.wikipedia.org/wiki/Nuclear_umbrella
[8] http://www.nato.int/cps/en/natolive/official_texts_17120.htm

Although it is possible to argue that these supervisory bodies have a limited ability to truly supervise the nuclear capabilities of the different states, these mechanisms are in place and working. Cyber supervision capabilities are currently nonexistent and it is doubtful that this type of supervision capability can be developed. What may be possible, however, is to develop the ability to cyber "quarantine" a country, not unlike the sanctions made on nuclear aspiring states today.

Summary

Throughout this article, we have tried to distinguish between nuclear and cyber technologies in order to provide a comparable analysis of these fields. The aim of this article is to discuss whether cyber weapons should be addressed in the same manner as nuclear weapons. It is clear that the answer is no. Even when analyzing terminology, nuclear weapons are well defined and cyber weapons are far from it.

When we take a look at the main points we have discussed we discover that:

- There are **no indicators of cyber attacks.** Consequently, because they can get away with it there is no disincentive for countries or non-state actors to launch cyber attacks.
- Some non-state actors have **better monitoring abilities** than states (Microsoft, Google, etc).
- **There are no means to supervise or control the manufacturing of cyber weapons**.
- Stakeholders are not only countries but also non-state organizations and criminal organizations.
- There are no real budget barriers to creating cyber-attack weapons.
- Since cyber weapons are so “handy” and readily available to everyone. They are difficult to trace and have a great “potential”. In the near future **we will see a significant rise in the quality of the attacks** and an increase in the damage caused.

To take this reasoning a step forward, we can infer that cyber weapons are not and should not be treated as nuclear weapons. It is true that in some cases, the damage attributed to cyber weapons can justify retaliation by WMD but these are the extreme cases. There have been those that tried to use existing treaties and tools as a means of controlling cyberspace and cyber weaponry. However, as we have shown in this article, the cyber world is a brave new one. Where old, true and tried, measures will probably cause more damage than good. New concepts should be adopted when discussing cyber technologies and with them new measurements and tools to control cyber weapons.

Summary table

Metric	Nuclear Weapons	Cyber Warfare	Conclusion
Countries / Users Attributes			
Ability to Manufacture	States	Amateurs and up	No means to supervise or control the manufacturing of cyber weapons. Stakeholders are recognized as not only countries but also "Non-State" organizations and crime elements.
Ability to Maintain	High yield weapons – States only (Delivery device is needed)	Everybody. Internet is sufficient delivery.	Short term attacks – Easily maintained and conducted. Long term attack – Investment in people, knowledge and money is needed.
Second Strike Capability	Available after the development of sufficient delivery capability	Available after the development of sufficient delivery capability – The enemy can target this ability using first strike, which makes this a prime target.	Due to the many unknowns in a cyberattack (both in measures of signature and agility) second strike sometimes cannot be launched against the attacker. And when launched can sometimes be ineffective.
Technological Maturity	Physics, Mathematics, Material Sciences, Aeronautic Engineering and much more at a very high level	Computer sciences at a very low level	There is no technological barrier to the creation of a simple cyber attack. Furthermore, cyberattacks can be Purchased "Off the Shelf"
Budgetry Constraints	High	Low	There is no budgetary barrier to the creation ofi a simple cyber attack.
Weapon Attributes			
Previous use and consequence	Hiroshima and Nagasaki, Chernobyl – High mortality rates and loss of property	Estonia, Georgia, China – Google (?), China – US (?), Ghostnet (China ?), 4th of July attacks (N. Korea), other un-reported incidents	No cyber attack has been accountable for the death of thousands/millions of people. There is no milestone in the "cyber" history that proves the ability of a cyber-attack to create such damage.
Indicators	Radiation, Technology purchase, infrastructure	Almost none. The in-house ability to train and field "cyber-warriors"?	There are no disincentives for countries or non-sate actors to use cyber weapons.. Countries can get away with attacks that are not possible in the physical world. Some non-state actors have monitoring abilities larger than countries (Microsoft, Google, etc).
Use-Case Scenarios	War, Terrorism ("Dirty" bombs)	War, Espionage, Terrorism, Anarchism, Hacktivism	Cyber weapons are much broader than nuclear weapons and are used on a day-to-day basis.
Control over pyload and consequence	Complete control over Payload, High level of reliability in consequence	Complete control over Payload, low level of reliability in consequence	The ability to estimate the consequence of a cyber attack is limited at best, and composed of guesses at worst.
Source Signature	Easy, unless in the case of "Dirty Bombs"	Hard, almost impossible in current Internet environment	The ability to use proxies is unheard of in the case of nuclear weapons, limiting the ability to identify an attacking entity.
Primary and Secondary effects of the Weapon			
Damage Capability	WMD	Damage to equipment, damage to "way of life",	The damage capability of a large, effective cyber attack is yet to be seen.

		damage to auxiliary systems. Far end scenario – Fatalities	
Long Term Effects	Nuclear fallout (intended / not intended)	Loss of data, loss of confidence (?)	When looking at previous cyber attacks, it is uncertain that there is any long term effect.
Unintended Consequences & Cascading Effects		Auxiliary systems shutdown. Critical system cascading effect. Relying systems shutdown.	
Stealth Ability	Non existent	A skilled team can create a stealthy attack.	
International Treaties & Supervision			
International Cooperation to prevent usage	Solid, established for years.	Not present, some basic "weak" conventions to handle underlying issues	Due to the lack of ability to prove the actual involvement of countries, such treaties are unenforceable and as such without actual force Effective international cooperation could happen at the Intelligence levels but this could only happen using bilateral treaties and not multilateral ones.
Proliferation	Heavily supervised. Very hard to proliferate due to storage and technological necessities	Easy, not supervised at all	Proliferation is done by e-mail or passing a thumb drive.
Protective Umbrella	Established in Bilateral and Multilateral agreements for years.	No Protective Umbrella established as of today	Limited ability to create a protective umbrella but for incident response and not deterrence.
Supervision Ability	Possible, big and efficient supervision bodies exists	Probably not possible.	Limited supervision possible, although very hard to achieve, usually at the cost of civil liberties.