UNIVERSITY OF Southampton

COMP6224 (2016)
week 6: cyber warfare

Vladimiro Sassone

Cyber Security Centre

University of Southampton

cybersecurity centre

GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

CyberSecuritySoton.org [w]

@CybSecSoton [fb & tw]

historic notes, or how did we get here

electronic warfare dates back to the days of telegraphs, radio & radars

1. denial of service (jamming, mimicry, physical attack);
2. deception (targeted at automated systems or at people);
3. exploitation (eavesdropping for operationally valuable information).

It aims at controlling the electromagnetic spectrum, to intercept, disrupt, locate, analyse, spoof, etc, enemy communications.

Defence involves not just protecting the authenticity and confidentiality of the content (straightforward by encryption and authentication) but also preventing traffic analysis, direction finding, jamming and physical destruction.

PART I: How did we get so far

information warfare

About in 1995 the phrase "*Information warfare*" came into use.

In Desert Storm one goal of NSA personnel supporting the allies was to enable the initial attack to be made without casualties — even though the Iraqi air defences were at that time intact and alert.

This involved a mixture of standard e-war techniques such as jammers and anti-radiation missiles; cruise missile attacks on command centres; attacks by special forces who sneaked into Iraq and dug up lengths of communications cabling from the desert; and, allegedly, the use of hacking tricks to disable computers and telephone exchanges.

The operation successfully achieved its mission of ensuring zero allied casualties on the first night of the aerial bombardment.

But in April 2007, it was thrust back on the agenda by events in Estonia… (more to follow about this…)

what is it meant by information warfare?

There are roughly three views on what information warfare means:

- a re-marketing of usual stuff to try and keep military budgets post-Cold-War;
- the use of ‘hacking’ in a broad sense to deny critical military and other services for operational or propaganda purposes;
- extension of electronic warfare doctrine to control all information relevant to the conflict, also incorporating propaganda and news management.

from information war to cyberwar (1)

United States 1982

In 1982, US President Reagan approved a CIA plan to transfer software used to run pipeline pumps, turbines, and valves to the Soviet Union. The software had a logic bomb designed to cause pump speeds and valve settings to malfunction. “The result was the most monumental non-nuclear explosion and fire ever seen from space.”

United States 1991

The US used cyberwarfare means and methods when it invaded Iraq in 1991.

Chechnya 1994 and 1997-2001

Pro-chechen and pro-russian forces waged a virtual war on the Internet, simultaneous to their conflict on the ground. The Chechen separatist movement in particular is considered a pioneer in the use of the Web as a tool for delivering powerful PR messages. Both sides used cyberspace to engage in information operations to control and shape public perception. In particular, digital images of bloody corpses served to turn public opinion against perceived Russian military excesses.

from information war to cyberwar (2)

Kosovo 1999

If Vietnam was the world's first TV war, Kosovo in 1999 was the first broad-scale Internet war. As NATO planes began to bomb Serbia, numerous pro Serbian or anti-Western hacker groups, such as the 'Black Hand,' began to attack NATO Internet infrastructure. Their stated goal was to disrupt NATO military operations.

The Israeli-Palestinian Cyberconflict July 1999 to April 2002

In September 2000, Israeli teenage hackers created a website to jam Hezbollah, Hamas and Palestinian National Authority websites via a sustained DDoS attack. This quickly escalated into an international incident.

Hackers struck 3 high-profile Israeli sites belonging to the Israeli Parliament, the Ministry of Foreign Affairs, and the Israeli Defense Force information site. Later, they also hit the Israeli Prime Minister's Office, the Bank of Israel, and the Tel Aviv Stock Exchange. By January 2001, the conflict had struck more than 160 Israeli and 35 Palestinian sites; 548 Israeli domain websites were defaced out of 2,295 in the Middle East.

The main types of attacks were website defacement and DDoS attacks

The Cyber Attack on Estonia April-May 2007

Estonia, with a population of 1.3 million people, has become a marvel in terms of widespread access and reliance on the Internet. This attracted the interest of Russian hackers.

When the Estonian government relocated the monument commemorating the Soviet armed forces' liberation of Estonia from the Nazi, a barrage of DDoS attacks (ranging from individuals using low-tech methods to expensive rentals of botnets) clogged Estonia's Internet network.

The websites of the Ministries of Foreign Affairs and Justice had to shut down, while Prime Minister's Party's website was defaced with digital graffiti of a Hitler-style moustache scrawled across the Prime Minister's photo. On 3 May, the botnets began attacking private sites and servers. Banks in Estonia were shutdown, save a few, but it came at great monetary costs and affected also international banking.

The Russian hacktivists also managed to briefly disable the national emergency toll-free phone number 112. Moscow denied any involvement in the attacks, but Estonian officials have reiterated their certainty that the Kremlin was behind the attacks.

from information war to cyberwar (4)

Chinese attacks against European government networks in 2007

The British Security Service, the French Prime Minister's Office, and the Office of German Chancellor complained to China about intrusions of their government networks. Merkel even raised the matter with China's President Hu Jintao. No official source in China has admitted complicity in these cases.

Israeli disruption of Syrian air defense networks 6 September 2007

Operation *Orchard* was an Israeli airstrike on a target in Syria carried out on 6 September 2007 that destroyed the Al Kibar complex with missiles and laser-guided bombs. In May 2008, a report in IEEE Spectrum cited European sources claiming that the Syrian air defense network had been deactivated by a secret built-in switch activated by the Israelis.

Lithuania June-July 2008

On 17 June 2008, the Lithuanian Parliament prohibited public displays of Soviet and Nazi German insignia and playing the Soviet and Nazi anthems. Hundreds of government and corporate websites in Lithuania were hacked, and some were covered in digital Soviet-era graffiti, implicating Russian nationalist hackers.

The Russia-Georgia War August 2008

The first example of cyberattacks that coincided directly with a land, sea, and air invasion, and probably the best example of how to use computer network attacks in a modern battle-space.

Russia invaded Georgia in response to Georgia's attack against the separatists in South Ossetia. The coordinated cyber campaign utilised vetted target lists of Georgian government websites and other strategically valuable sites, e.g. the US and British embassies. Russia and its sympathisers also disrupted key Georgian media sites with botnets and command and control systems through DDoS attacks, electronic warfare jamming technique, website postings and defacement.

Attack vectors included DDoS, SQL injection, and cross-site scripting XSS.Main targets were government websites, financial and educational institutions, business associations, and news media websites, among them BBC and CNN.

The strategic lesson learned is that cyber attacks are a viable military option on the battle-space. Another lesson is that cyber attacks can be launched from safe remote locations. And finally, that cyber attacks do not produce quantifiable results as consistently as kinetic strikes do. The tactical advantage for most offensive cyber attacks may go to the defender, because it is easier and faster to implement defenses than it is to develop offensive cyber attack techniques.

Kyrgyzstan January 2009

The attack focused on three of the four Internet Service Providers (ISP). The DDoS attack quickly overwhelmed the three ISPs and disrupted all Internet communications. The IP traffic was traced back to Russian-based servers primarily known for cybercrime activities. Multiple sources have blamed the attack on the Russian cyber militia and the Russian Business Network (RBN) suspected to control the world's largest botnet with between 150 and 180 million nodes.

Coordinated South Korean-US attacks July 2009

A series of DDoS attacks began to strike first South Korean and then both South Korean and US government and commercial websites. Investigations revealed a botnet together with rudimentary DDoS attacks such as HTTP request floods, UDP, and ICMP floods. The targets, together with the timing between a North Korean missile test launch and the anniversary of Kim Il Sung's death led some to suggest that North Korea was behind the attacks. To date, there is no evidence of this.

Cyber attacks against Iranian nuclear facilities from 2009 to 2010

A cyber worm called 'Stuxnet of unknown origin, developed and released in a number of countries in 2009, has damaged cascades of centrifuges, illegally obtained and operated in a highly protected site at Natanz, in Iran.

Stuxnet is a sophisticated weapon. Its estimated cost is in excess of $10m, which points straight to state actors. It contained a large number of zero-day exploits, which are not so common and expensive. It attacks and disables nuclear centrifuges that operate with a SCADA system of the Siemens type, overriding the proprietary software and overloading the centrifuges. The latter so cleverly, that it disguises the damage in progress from operators and overseers until too late to reverse.

A video on Stuxnet / A TED presentation from Ralph Langner.

We shall get back to Stuxnet.

more considerations on Stuxnet

Stuxnet achieved pretty much what air strikes would have achieved, only at much less cost, without known fatalities, and without a full-blown war in the Middle East.

The cost of development of Stuxnet has been estimated to be around $10 million. The cost of air strikes would have been multiple, only counting material, not fatalities and injuries. Several fighter jets would have been lost in a campaign against Iran. And there would have been many dead and many injured, significant destruction by Iranian missiles fired in retaliation and a huge amount of collateral damage just by the oil price jumping. In military terms, it was a bargain.

However, the attack's overall effect was impressive. Iran has replaced all of its damaged centrifuges and has resumed enriching uranium. This suggests that cyber-weapons are not the '*silver bullet*' replacement for traditional military instruments that they have been purported to be. It has not coerced Iran into abandoning that program.

Stuxnet also shows that effective cyber attacks require large, complex operations, and entail a massive intelligence burden. And there is another problem: cyber weapons can be copied and their proliferation cannot be controlled. Stuxnet-inspired weapons and technology may soon be in the hands of rogue nation-states, terrorists, organised crime, and hackers.

but how can a virus cripple a nation?

We shall say more about Stuxnet, for the moment let's stop to reflect on how it seems to mark a very different class of attack:

Stuxnet is a proper cyber weapon, which can cripple and seriously damage a nation. There are serious doubts that any of the other episodes constitute acts of war (more like "cold war" perhaps). Here there are fewer doubts.

PART II: What is Cyberwar, actually?

what does this all mean?

Here are a few "take-aways" from the story so far.

Cyber war is real. What we have seen so far is far from indicative of what can be done. Most of these skirmishes in cyberspace used primitive cyber weapons. One could reasonably guess that what the some nations are capable of doing in a cyber war could devastate a modern nation.

Cyber war is fast. As the photons of the attack packets stream down fibre-optic cable, the time between the launch of an attack and its effect is barely measurable, thus creating risks for crisis decision makers.

Cyber war is global. Cyber attacks rapidly go global, as covertly acquired or hacked computers and servers throughout the world are kicked into service.

Cyber war skips the battlefield. Systems that people rely upon, from banks to air defence radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defences.

Cyber war armament has begun. Nations are "preparing the battlefield." They are hacking into each other's networks and infrastructures, laying in trapdoors and logic bombs—now, in peacetime. This ongoing nature of cyber war, the blurring of peace and war, adds a dangerous new dimension of instability.

Cyber war uses the same tools as hackers, hacktivists, cyber criminals, …

yet, is it cyberwar or just more of the same?

Whilst everybody agrees that cyber techniques will be used in any conflict, not everybody agrees though that there is a cyberwar going on at the moment.

There's a power struggle going on in the U.S. government right now.

It's about who is in charge of cyber security, and how much control the government will exert over civilian networks. And by beating the drums of war, the military is coming out on top.

Bruce Schneier (read relevant blog entry)

(here is a TV debate about the issue)

A lot of this is about fine points in the use of language. But a real questions is: Can there be a cyber-only war?

but what is (cyber)war then?

Whether it be war on land, at sea, or in the air, or in cyberspace, war always has a *political goal* and *mode* (which distinguishes it from crime) and always has an element of *violence*.

Currently, the understood legal stance is that to meet this definition of the *use of force*, a cyberattack would have to

> "proximately result in death, injury or significant destruction."

That is, even if conducted through cyber means, the effect must be physical damage or destruction. To provide a parallel, a plane dropping bombs is engaged in air warfare; a plane dropping leaf- lets, not so much.

there is no clear agreement yet

During the Russian attack, Estonia's called for help, arguing that NATO was obliged to defend a member state against this start of a new "cyberwar." NATO didn't think so: Estonia was being bullied in cyberspace, but no one was dead or hurt and no property was actually destroyed or damaged.

The way to determine when a cyberattack constitutes the kind of "use of force" that legally justifies war is to weigh its effects. What did the act do to the real world? The severity of the attack is not the only thing. All sorts of actions that could ultimately spark a chain of events that cause the same death and destruction as traditional war.

> "*We tend to think of war and peace as an on-off toggle switch. The reality is that are in a constant state of conflict among nations that rarely gets to open warfare. Countries like China — with which we are certainly not at war— are in intensive cyberconflict with us.*"
>
> Joel Brenner, former head of counterintelligence US Director of National Intelligence.

Cyberwar has more in common with informal concepts of conflict like the Cold War.

The USA view on cyberwar

Do you know what “9ec4c12949a4f31474f299058ce2b22a” means?

This code appears in the logo of the US military’s Cyber Command, a revolutionary new military organization formed in 2010. It’s the MD5 hash of their mission statement:

> *“USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks; and prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.”*

Cyber Command brings together all components of the US military that work on cyber issues, a cyber warrior force of just under 60,000 personnel.

The strategy that guides CYBERCOM draws from the overall idea that cyberspace is a new domain of both possibilities and risks, and the US military must protect its “freedom of maneuver” and establishing “dominance”.

The USA view on cyberwar

UNIVERSITY OF Southampton

Do you know what “9ec4c12949a4f31474f299058ce2b22a” means?

This code appears in the logo of the US military’ Command, a revolutionary new military organization formed in 2010. It’ their mission statement:

> *“USCYBERCOM plans, coordinates, integ ts activities to: direct the operations and defense of specified I n networks; and prepare to, and when directed, conduct operations in order to enable actions in all domains, ensure US pace and deny the same to our adversaries.”*

Cyber Command brings together all com ary that work on cyber issues, a cyber warrior force of just u nnel.

The strategy that guides CYBERCOM draws from the overall idea that cyberspace is a new domain of both possibilities and risks, and the US military must protect its “freedom of maneuver” and establishing “dominance”.

China's view on cyberwar (1)

Unsurprisingly, Chinese writers and officials have reacted angrily to direct and veiled accusations, describing them as "groundless and reflecting Cold War mentality."

They assert that the aggrieved party is China. By the raw numbers, China suffers the largest number of cyberattacks in the world. Government officials claimed that in 2012 Chinese military sites alone were targeted by American sources almost 90,000 times.

Far from taking the blame for cyber insecurity (the high malware infection rate arises because as much as 95% of software in China is pirated), China's position is to equip itself for future cyberthreats and conflicts.

> "*Of late, an Internet tornado has swept across the world massively impacting and shocking the globe. Behind all this lies the shadow of America. Faced with this warm-up for an Internet war, every nation and military can't be passive but is making preparations to fight the Internet war.*"

China's view on cyberwar (2)

In real terms, this has translated into a buildup of the People's Liberation Army's (PLA) cyber capabilities at just as rapid a pace as the building out of Cyber Command and the NSA over the same period.

The Chinese plan for cyber war would most likely focus on defending PLA networks and, in turn, targeting the adversary's key nodes of communication, command, and coordination.

The idea is to degrade an enemy's decision-making, slow down its operations, and even weaken its morale. The basic thinking is that any foreign power that might threaten China (i.e., the United States) would depend on well-coordinated technical systems. Infiltrating and disrupting these systems is thus a natural "defensive" posture.

Unfortunately, to those on the opposite end of the cyber gun barrel, the emphasis on infiltrating and disrupting communications and command systems looks aggressive.

a few definitions for a more precise view

UNIVERSITY OF Southampton

Cyber attacks by *hackers* take place regularly, much more frequently than state-sponsored activities. Some hackers are state-sponsored and perform lawful activities, but some are not. What determines the legality of these operations is intent.

Cyber vandalism is '*cyber hacktivism*,' which is a common term for hackers who use illegal digital tools in pursuit of political ends.[4]

Cybercrime or Internet crime, undertaken for criminal gain, is taking place regularly and independently of conflicts. Yet, Cybercrime provides an environment in which attack techniques can be refined: "It is the laboratory where the malicious payloads and exploits used in cyber warfare are developed, tested, and refined."

Cyber espionage is a routine occurrence and an expansion of traditional efforts to collect information on an opponent's secrets, intentions, and capabilities. It consists of the search for access to classified, personal or corporate data, intellectual property, proprietary information and patents, or results from research and development projects, for reconnaissance, probing, and testing of ICT defenses, and clandestine manipulation of data, information and critical infrastructure for war preparation.

more definitions (1): cyberpower

In the military doctrine, Cyberspace, the novel 5th domain after land, sea, air, and space, is all of the computer networks in the world and everything they connect and control via cable, fibre-optics or wireless.

Power based on information resources is not new; *cyberpower* is:

> *"cyberpower is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."*

Cyberpower has three characteristics: it is *ubiquitous*, *complementary*, and can be *stealthy*.

Land, sea, air, and space power are able to generate strategic effect on each of the other domains. But nothing generates strategic effect in all domains so absolutely and simultaneously as cyberpower, because cyberpower is *ubiquitous*.

The coercive ability of cyberpower is currently limited. Eg shutting down a power grid via cyberpower may have catastrophic consequences. But rather than coercing its victim to concede to an attacker's demands, it may invite an even more catastrophic response. Thus, until cyberpower will prove its coercive capability, it is a *complementary instrument*.

That cyberpower can be *stealthy* makes it attractive to many users. They can use this ability to wield it surreptitiously on a global scale without it being attributable to the perpetrator.

more definitions (2): acts-of-war

UNIVERSITY OF Southampton

War is the *use of force* to cause damage, destruction or casualties for political effect by states or groups. The grey area consists of disruption of data and services *below the level of use of force.* The threshold for regarding a cyber incident as the use of force is the most important *ambiguity* in cyberwar.

The *right of self-defence* is triggered by the use of force: only large scale cyber attacks on critical infrastructures that result in significant physical damage or human losses comparable to those of an armed attack with conventional weapons would entitle the victim state to invoke self-defence.

There is consensus based on international practice that propaganda, harassment, hacktivism, and crime are *not acts of war* and *do not justify the use of force in response.* But other areas are less clear. Eg, are *intelligence collection* or *cyber reconnaissance* acts of war? Nondestructive computer methodologies used for cyber espionage may violate the domestic law of the victim nation-state but are *not contrary to international law*.

Ultimately, the decision as to whether something is an act of war is a political decision. “The answer to whether a particular attack is an act of war comes down to this: is it in your interest to declare it so?”

more definitions (3): means/vulnerability

UNIVERSITY OF Southampton

Although there is no universally accepted definition of cyber warfare, according to a general definition

> "*cyber warfare refers to a massively coordinated digital assault on a government by another. It is the action by a nation-state to penetrate another nation's computers and networks for the purposes of causing damage or disruption*."

Confusion arises as the term is often used informally to describe attacks between corporations, from terrorist organisations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent.

A successful cyberwar depends upon two things: *means* and *vulnerability*.

The 'means' are the people, tools, and cyber weapons available to the attacker.

The 'vulnerability' is the extent to which the enemy economy and military use the Internet and networks in general.

cyber warfare capabilities of main actors

Nation	Cyber Offence	Cyber Dependence	Cyber Defence	Total
USA	8	2	1	11
Russia	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
North Korea	2	9	7	18

source: Richard A. Clarke (table based exclusively on individual perception)

former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States; now analyst and novelist

more definitions (4): jus in bello

Once a state has entered into a conflict, the use of force is governed by *jus in bello*, governed by six principles.

(1) military necessity, (2) distinction, (3) proportionality,
(4) perfidy, (5) neutrality, (6) unnecessary suffering

1. international humanitarian law restricts the use of force to targets that will accomplish valid military objectives.
2. the parties to a conflict must "at all times distinguish between the civilian population and combatants, and between civilian objects and military objectives."
3. governs the degree and kind of force used to achieve a military objective by comparing the expected military advantage gained to the expected incidental damage to civilians and property.

more definitions (4): jus in bello

Once a state has entered into a conflict, the use of force is governed by *jus in bello*, governed by six principles.

(1) military necessity, (2) distinction, (3) proportionality,
(4) perfidy, (5) neutrality, (6) unnecessary suffering

4. the parties to a conflict must *not cross the line into perfidy*. Eg, tricking enemies to believe that combat vehicles of the opponent were medical vehicles would be perfidious. Perfidious conduct would be firing on an adversary raising the flag of surrender and coming from cover.
5. permits a state to declare itself neutral. An attack through a network that crosses neutral territory, or uses a neutral's satellites, computers, or networks, would infringe neutrality. Conversely, a neutral's failure to resist the use of its networks for attacks against another country makes it a legitimate target for reprisals.
6. prohibits the use of weapons designed to cause unnecessary suffering: harm should be no greater than is necessary to achieve legitimate military objectives.

global trends (1): increase vulnerability

Two global trends, while providing greater efficiency and better services, increase vulnerabilities and the consequences of security failures.

Network convergence: the merging of distinct voice and data technologies to a point where all communications are transported over a common network structure. This amplifies the opportunity for, and the consequences of, disruptive cyber attacks and unforeseen effects on other parts of the critical infrastructure.

Channel consolidation: the concentration of data captured on individual users by service providers, which increases the potential and consequences for exploitation of personal data by malicious actors.

global trends (2): networked forces

The Internet has enabled the most recent military innovation: *networked forces.*

"*Bombs are guided by GPS satellites; drones are piloted remotely from across the world; fighter planes and warships are now huge data-processing centres; even the ordinary foot-soldier is being wired up*."

Weapon systems are ever more dependent on software, computer hardware, and battle-space networking.

Eg, in the past, 100% of an aircraft's performance and capabilities were defined by hardware. In recent advanced aircraft, 75+% of performance and capability is dependent on software. Without software, some aircraft would not be controllable.

For instance, the F-16 is unstable below Mach one, and uncontrollable without its software-based flight control system. The Boeing 777 and the Airbus 330 have software flight control systems without any manual backup

computer network operations

From this point of view, Cyberwar is a warlike conflict in virtual space with means of ICT and networks. It aims at influencing the will and decision making capability of the enemy's political leadership and armed forces in the theatre of *Computer Network Operations* (CNO). Tree forms of CNO can be distinguished:

1. *Computer Network Attack*, disrupt, deny, degrade, or destroy information resident in computers and networks, or the computers or networks themselves;
2. *Computer Network Exploitation*, retrieve intelligence-grade data and information from enemy computers by ICT means; and
3. *Computer Network Defence*, which consists of all measures necessary to protect own ICT means and infrastructures against hostile computer network attacks and exploitation.

Because cyber security is evolving from a technical discipline to a strategic concept, and because cyber attacks can affect national security at the strategic level, national leaders must look beyond the tactical arena: *the quest for strategic cyber security involves marshalling all of the resources of a nation-state.*

cyber warfare vs information warfare

In most countries *Cyberwar* is seen as a part of *Information Warfare*, which as discussed before is broader and banks on five core capabilities:

(1) Psychological Operations, (2) Military Deception, (3) Operations Security,
(4) Computer Network Operations, and (5) Electronic Warfare.

Defined as "the integrated employment of these core capabilities to influence, disrupt, corrupt, usurp adversarial human & automated decision-making while protecting the own"

- *Psychological Operations* (PSYOP) planned operations to convey selected information to targeted foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organisations, groups, individuals.
- *Military Deception* (MILDEC) guides an enemy into making mistakes by presenting false information, images, or statements. Deception is defined as "actions executed to deliberately mislead adversary military decision-makers thereby causing them to take specific actions that will contribute to the success of friendly military operations."
- *Operations Security* (OPSEC) is a process of identifying information that is critical to friendly operations and which could enable adversaries to attack operational vulnerabilities.
- *Computer Network Operations* (CNO) include the capability to attack and disrupt computer networks, defend the own information and communications systems, and exploit enemy computer networks through intelligence collection, usually done through use of computer code and computer applications.
- *Electronic Warfare* (EW) is defined as any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy.

information assurance and dominance

Information Assurance (IA) consists of protecting and defending information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation.

Intelligence is the enabler to military dominance of Information Operations.
Coupled with Command and Control Warfare leads to *Information Dominance*, which may be defined as superiority in the generation, manipulation, and use of information sufficient to afford its possessors *military dominance*. It has three sources:

- *Command and Control,* permits everyone to know *where* they and their cohorts are in the battle-space, and enables them to execute operations *when* and *as quickly as* necessary
- *Intelligence,* ranges from knowing the enemy's disposition to knowing the location of enemy assets in real-time with sufficient precision for precision kills.
- *Information Operations,* confound enemy information systems at various points – sensors, communications, processing, and command – while protecting one's own.

cyber weapons

For reference, a missile is comprised of three basic elements:

1. a *delivery vehicle*, the rocket engine,
2. a *navigation system,* which tells it how to get to the target, and
3. the *payload*, the components that cause harm.

The same three elements appear in the design of a cyber weapon.

There are numerous methods of delivering cyber weapons to their targets. As we have already seen, they include: emails with malicious code embedded or attached; websites with malicious links and downloads; wireless code insertion transmitted over radio or radar frequencies. Hacking is a *manual delivery vehicle* that allows placing the malicious payload on a target computer, system or network. Counterfeit hardware, software, and electronic components can also be used as delivery vehicles.

The *payload* of a cyber weapon could be a program that copies information off of the computer and sends it to an external source. It can also be a program that is altering and manipulating information stored on the system. Finally, it can enable remote access so that the computer can be controlled or directed over the Internet.

what can be attractive in cyberwar? (1)

- Cyberwar is cheaper since it does not require large numbers of troops and weapons.
- Entry costs are low: with a computer and Internet anyone can engage in cyberwar.
- Cyberwar is easy to deliver by stealth via global connectivity from anywhere.
- Tools for attack are cheap and openly available on the Internet.
- The proliferation of such tools happens without any control.
- The attacker who can profit from the latest and newest innovations.
- Cyberspace offers the attacker anonymity, as it is hard to trace the origin of attacks.
- Cyberspace gives disproportionate power to small and relatively insignificant actors.
- Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity, at least in the short term.
- Helps avoid the need to engage in combat operations and thus saves lives.
- Leads to the ability to disrupt the adversary rather than destroy his forces.

what can be attractive in cyberwar? (2)

UNIVERSITY OF Southampton

- Blurred traditional boundaries: Cyber warfare creates its own ‘fog and friction of war.’
- Cyberwar enables actors to achieve political and strategic goals without armed conflict.
- Cyberwar skips the battlefield. Systems that people rely upon, from banks, the electric power grid to air defence radars, are accessible worldwide from cyberspace and can be quickly taken over or knocked out without first defeating a country’s traditional defences.
- Cyberwar happens at almost the speed of light. As photons of attack packets stream down fibre-optic cables, the time between the launch of an attack and its effects is barely measurable, thus creating more risks for decision makers, particularly in a crisis.
- The victim of an attack has to invest considerable resources into neutralising the threat, which requires teams of dedicated software and hardware experts with specific skill sets. Such persons are difficult to recruit and to retain as private industry offers more attractive terms for their talent.
- The vulnerabilities of countries increasingly dependent on complex, interconnected, and networked information systems increase over time, thus providing adversaries with a target rich environment.

the problem of attribution and deniability

Unlike nuclear or other weapons of mass destruction, cyber weapons and cyber attacks require little infrastructure, no restricted materials nor knowledge which is in short supply. Cyber weapons are easy to obtain and to use, and become ever more powerful and sophisticated.

Attribution –determining the source, location, and the identity of an attacker– is extremely difficult for both technical and nontechnical reasons.

Electrons do not bear national markings. The Internet has no reliable means for tracing where a message comes from. The Internet was not designed to withstand malicious alteration of the transmission packets

To attribute an attack with any measure of certainty to a specific device, let alone a specific individual or entity, is *virtually impossible*.

So, attackers enjoy a formidable advantage: *anonymity.* Smart hackers hide within the maze-like architecture of the Internet. Those with sufficient technical skill can remain anonymous at will.

Plausible deniability is also a concern. Because hackers obscure the true origin of an attack by hopping through a series of compromised computers to reach their target, the attacker can always claim that his computer had been hacked and used in someone else's operation.

the problem of cyber deterrence

UNIVERSITY OF Southampton

Cyber warfare is a great equaliser and a new form of asymmetrical warfare which is tempting to take. Yet, as long as secure passive cyber defence is impossible, deterrence seems the only feasible path.

The problem is that *cyber deterrence* does not work as well as nuclear deterrence. In fact, deterrence is pointless without attribution: if retaliation does not hit the attacker, he will not be deterred. And retaliation against the wrong actor is unjust and a crime of war.

States have two possible deterrence strategies: *denial* and *punishment*. In cyberspace, both suffer lack of *credibility*. To deny to have cyber weapons in not credible, given the availability of the technology and the lack of international legal frameworks. To threat punishment is not credible, because of the attribution problem and of cyber asymmetry.

For cyber deterrence to work effectively, we need a comprehensive scheme of *offensive* and *defensive* cyber capabilities balancing out.

common methods of cyber attack (1)

UNIVERSITY OF Southampton

Denial-of-Service Attacks

Flooding:	Sending extraneous data or replies to block a host service
Synchronize/reset flooding:	Exploiting limited cache in IP stack to block connections
Smurfing:	Using the IP broadcast system and IP spoofing to multiply floods
Out of band/fragment attacks:	Exploiting vulnerabilities in IP stack kernel implementations
Nuking:	Using forged messages to reset active connections
Specific denial of service:	Generating requests that block one specific vulnerable service

Malicious Software Attacks

Backdoor:	Program feature allowing remote execution of arbitrary commands
Worm:	Program that spawns and spreads copies of itself
Virus:	Code that self-reproduces in existing applications
Trojan:	Program-in-a-program that executes arbitrary commands

Exploiting Vulnerabilities

Access permissions:	Exploiting read or write access to system files
Brute force:	Trying default or weak login/password combinations
Overflow:	Writing arbitrary code behind the end of a buffer and executing it
Race conditions:	Exploiting temporary, insecure conditions in program

common methods of cyber attack (2)

UNIVERSITY OF Southampton

IP Packet Manipulation

Port spoofing:	Using commonly used source ports to avoid filtering rules
Tiny fragments:	Using small packets to bypass firewall protocol/port/size checks
Blind IP spoofing:	Changing source IP to access password services without a password
Name-server ID “snoofing”:	Blind spoofing with calculated false ID numbers name-server-caches
Sequence-number guessing:	Calculating TCP sequence and number to spoof a trusted host
Remote-session hijacking:	Using spoofing to intercept and redirect connections

Insider Attack

Backdoor daemons:	Opening a port for further remote access
Log manipulation:	Removing traces of attacks and unauthorised access
Cloaking:	Replacing system files to hide unauthorised access
Sniffing:	Monitoring network data to find sensitive data (e.g. passwords)
Nonblind spoofing:	Monitoring network to hijack active or to make forged connections

attack classification

UNIVERSITY OF Southampton

Passive attack

Passive attacks include analysing traffic, monitoring unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information (e.g., passwords). Passive intercept of network operations can give adversaries warnings of impending actions. Passive attacks can result in disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active attacks

Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. These attacks may be mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorised remote user during an attempt to connect to an enclave. Active attacks can result in the disclosure or dissemination of data files, denial of service, or modification of data.

Close-in attacks

Close-in attack consists of a regular individual's attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry, open access, or both.

Insider attacks

Insider attacks can be malicious or non-malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorised users. Non-malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as "getting the job done."

Distribution attacks

Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code, such as a backdoor, into a product to gain unauthorised access to information or a system function at a later date.

summary of part II

UNIVERSITY OF Southampton

- Cyber threats pose critical national and *economic security* concerns due to the rapid advances in, and increasing dependency on, ICT underpinning ever more aspects of modern society and life.
- The impact of this evolution can be seen in the *increasing scope of cyber security incidents*, and in the expanding range of actors and targets. However, by far not all such cyber security incidents qualify as cyber attacks. Cyber attack refers to *deliberate actions* to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems and networks.
- Cyberspace operations for the most part do not meet the criteria for '*use-of-force*' or '*act-of-war*' as currently defined by international law.
- The availability of cyber attack technologies for national purposes greatly *expands the range of options* available to national policymakers as well as those of other countries.
- The *consequences* of a cyber attack may be both *direct and indirect*, and in some cases of interest, the indirect consequences can far outweigh the direct consequences.
- States which are *highly dependent on* the capabilities afforded by ubiquitous *ICT* in every sector, both military and civilian, have *much to lose* from unrestrained cyber attacks that proliferate worldwide.
- While doubts remain as to whether strategic cyberwar is feasible, it is unlikely that a war would be fought *only with cyber weapons* and *purely within the cyber domain*.
- Like earlier technological innovations, these will be used to *degrade enemy capabilities* and to *shape the battle-space*, and perhaps *reshape the ways wars will be fought*.

PART III: Advanced Persistent Threat

"**China's economic espionage** has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy.

Beijing is waging a massive trade war on us all, and we should band together to pressure them to stop. Combined, the United States and our allies in Europe and Asia have significant diplomatic and economic leverage over China, and we should use this to our advantage to put an end to this scourge."[1]

— U.S. Rep. Mike Rogers, October, 2011

"**It is unprofessional** and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence."[2]

— Chinese Defense Ministry, January, 2013

APT and APT1

APT stands for "*Advanced Persistent Threat*". It refers to groups of advanced hackers characterised by the "persistency" and determination of their attacks. Once established within a network, APT groups will continually repeat the cycle of conducting reconnaissance, identifying data of interest, moving laterally to access that data, and "completing mission" by stealing the data. This will generally continue indefinitely until they are removed entirely from the network.

APT1 is the first and most successful of such groups. It is believed to be the

2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as unit 61398 (61398部队).

- APT1 has systematically took hundreds of terabytes of data from at least 141 organisations, and has demonstrated the capability and intent to steal from dozens of organisations simultaneously.
- APT1 maintains an extensive infrastructure of computer systems around the world.
- The size of APT1's infrastructure implies a large organisation with hundred, potentially thousands of human operators.

the alleged position of APT1 in PLA

FIGURE 1: Unit 61398's position within the PLA[11]

geographic activity of APT1

APT1 attack lifecycle

APT1 has a well-defined attack methodology, honed over years and designed to steal massive quantities of intellectual property. They begin with aggressive spear phishing, proceed to deploy custom digital weapons, and end by exporting compressed bundles of files to China – before beginning the cycle again.

initial compromise

The Initial Compromise stage represents the methods that intruders use to penetrate a target organisation's network.

Most common method is *spear phishing*.

Also, may send malicious content via social networking sites or instant messaging.

Another common tactic is strategic web compromise, in which the attacker places malicious code on websites that people in targeted organisations will likely visit.

May also look for vulnerable Internet-facing web servers and upload webshells in order to gain access to a targets internal network.

```
Date: Wed, 18 Apr 2012 06:31:41 -0700
From: Kevin Mandia <kevin.mandia@rocketmail.com>
Subject: Internal Discussion on the Press
Release

Hello,
Shall we schedule a time to meet next week?
We need to finalize the press release.
Details click here.

Kevin Mandia
```

initial compromise

The Initial Compromise stage represents the methods that intruders use to penetrate a target organisation's network.

Most common method is *spear phishing*.

Also, may send malicious content via social g.

Another common tactic is strategic web cor s malicious code on websites that people in targeted or

May also look for vulnerable Internet-facing order to gain access to a targets internal network.

```
Date: Wed, 18 Apr 2012 06:31:41 -0700
From: Kevin Mandia <kevin.mandia@rocketma
Subject: Internal Discussion on the Press
Release

Hello,
Shall we schedule a time to meet next weel
We need to finalize the press release.
Details click here.

Kevin Mandia
```

multi-hop access

Not easy firewall out dangerous IPs

FIGURE 21: APT1 bounces through "hop point" systems before accessing victim systems

establish a foothold

Ensures that group can access and control one or more computers within the victim organisation. APT1 utilises public backdoors (*Gh0st RAT* and *Poison Ivy*), “underground” backdoors found in hacker websites, and most often “custom” backdoors that they developed themselves.

These backdoors usually establish an outbound connection from the victim network to a computer controlled by the attackers. The communication methods used by the backdoors vary from clear text or simple encoding to the use of more advanced encoding or encryption. The backdoors will give the APT groups basic access to a system, typically through a command shell or graphical user interface.

FIGURE 17: Backdoors installed on compromised systems usually initiate connections with C2 servers

beachhead backdoors

Beachhead backdoors are typically minimally featured. They perform simple tasks like retrieve files, gather basic system information and trigger the execution of other more significant capabilities such as a standard backdoor.

APT1's beachhead backdoors are usually what we call *WEBC2 backdoors*.

A WEBC2 backdoor is designed to retrieve a webpage from a C2 server and will attempt to interpret the data between the special HTML tags as commands.

Typical sets of commands of beachhead backdoors:

- Open an interactive command shell (usually Windows' cmd.exe)
- Download and execute a file
- Sleep (i.e. remain inactive) for a specified amount of time

standard backdoors

The standard, non-WEBC2 APT1 backdoor typically communicates using the HTTP protocol (to blend in with legitimate web traffic) or a custom protocol that the malware authors designed themselves. These backdoors give APT intruders a laundry list of ways to control victim systems, including:

- Create/modify/delete/execute programs
- Upload/download files
- Create/delete directories
- List/start/stop processes
- Modify the system registry
- Take screenshots of the user's desktop
- Capture keystrokes
- Capture mouse movement
- Start an interactive command shell
- Create a Remote desktop (i.e. graphical) interface
- Harvest passwords
- Enumerate users
- Enumerate other systems on the network
- Sleep (i.e. go inactive) for a specified amount of time
- Log off the current user
- Shut down the system

the biscuit backdoor

UNIVERSITY OF Southampton

TABLE 4: A subset of BISCUIT commands

Command	Description
bdkzt	Launch a command shell
ckzjqk	Get system information
download <file>	Transfer a file from the C2 server
exe <file> <user>	Launch a program as a specific user
exit	Close the connection and sleep
lists <type>	List servers on a Windows network.
ljc	Enumerate running processes and identify their owners.
sjc <PID>|<NAME>	Terminate a process, either by process ID or by process name.
upload <file>	Send a file to the C2 server
zxdosml <input>	Send input to the command shell process (launched with “bdkzt”).

also try to disguise communication with C2 as

TABLE 5: Backdoors that mimic legitimate communication protocols

Backdoor	Mimicked protocol
MACROMAIL	MSN Messenger
GLOOXMAIL	Jabber/XMPP
CALENDAR	Gmail Calendar

escalating privileges

Acquires items that allow access to more resources within the victim environment.

Most often obtaining usernames and passwords. Also gaining access to PKI certificates, VPN client software, privileged computers, or other resources required to access data or systems of interest.

Typically accomplished by first "*dumping*" password hashes and "*crack*" them. Alternately, may leverage the hashes themselves in a "*pass-the-hash*" attack, where the hashed password itself may be used for authentication. A number of publicly available tools can be readily leveraged for both password dumping and pass-the-hash attacks.

escalating privileges

Acquires items that allow access to more resources within the victim environment.

Most often c to PKI
certificates, ces required
to access da

Typically acc ” them.
Alternately, r attack, where
the hashed p of publicly
available too d pass-the-
hash attacks

TABLE 6: Publicly available privilege escalation tools that APT1 has used

Tool	Description	Website
cachedump	This program extracts cached password hashes from a system's registry	Currently packaged with fgdump (below)
fgdump	Windows password hash dumper	http://www.foofus.net/fizzgig/fgdump/
gsecdump	Obtains password hashes from the Windows registry, including the SAM file, cached domain credentials, and LSA secrets	http://www.truesec.se
lsIsass	Dump active logon session password hashes from the lsass process	http://www.truesec.se
mimikatz	A utility primarily used for dumping password hashes	http://blog.gentilkiwi.com/mimikatz
pass-the-hash toolkit	Allows an intruder to "pass" a password hash (without knowing the original password) to log in to systems	http://oss.coresecurity.com/projects/pshtoolkit.htm
pwdump7	Dumps password hashes from the Windows registry	http://www.tarasco.org/security/pwdump_7/
pwdumpX	Dumps password hashes from the Windows registry	The tool claims its origin as http://reedarvin.thearvins.com/, but the site is not offering this software as of the date of this report

internal reconnaissance

UNIVERSITY OF Southampton

APT1 collects information about the victim environment using built-in operating system commands: internal network, computers, trust relationships, users, and groups.

Data of interest identified via directory or network share listings, or search for data by file extension, keyword, or last modified date. But most commonly consists of documents, the contents of user email accounts, or databases. Therefore file servers, email servers, and domain controllers are customary targets.

- » Display the victim's network configuration information
- » List the services that have started on the victim system
- » List currently running processes
- » List accounts on the system
- » List accounts with administrator privileges
- » List current network connections
- » List currently connected network shares
- » List other systems on the network
- » List network computers and accounts according to group ("domain controllers," "domain users," "domain admins," etc.)

```
@echo off
ipconfig /all>>"C:\WINNT\Debug\1.txt"
net start>>"C:\WINNT\Debug\1.txt"
tasklist /v>>"C:\WINNT\Debug\1.txt"
net user >>"C:\WINNT\Debug\1.txt"
net localgroup administrators>>"C:\WINNT\Debug\1.txt"
netstat -ano>>"C:\WINNT\Debug\1.txt"
net use>>"C:\WINNT\Debug\1.txt"
net view>>"C:\WINNT\Debug\1.txt"
net view /domain>>"C:\WINNT\Debug\1.txt"
net group /domain>>"C:\WINNT\Debug\1.txt"
net group "domain users" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain admins" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain controllers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange domain servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain computers" /domain>>"C:\WINNT\Debug\1.txt"
```

FIGURE 18: An APT1 batch script that automates reconnaissance

lateral movement

If the systems initially compromised do not contain the data that they want, APT1 moves laterally within a network to other computers that either contain that data or allow them to access it. Once they have a foothold inside the network and a set of legitimate credentials, it is simple to move around the network undetected:

» They can connect to shared resources on other systems

» They can execute commands on other systems using the publicly available "psexec" tool from Microsoft Sysinternals or the built-in Windows Task Scheduler ("at.exe")

These actions are hard to detect because legitimate system administrators normally use these techniques to perform actions around the network.

maintain presence (1)

Ensure continued control over key systems in the network eg by:

- install new backdoors
- install different families of malware on multiple computers
- use a variety of command and control addresses for redundancy and make it difficult to identify and remove all access points.

APT may establish methods of network access without backdoors, eg use of valid PKI/VPN credentials to masquerade as a legitimate user.

APT actors have been able to circumvent two-factor authentication to maintain access to a victim network and its resources.

maintain presence (2)

APT1 does this in three ways:

1. Install new backdoors on multiple systems

Throughout their stay in the network (which could be years), APT1 usually installs new backdoors as they claim more systems. Then, if one backdoor is discovered and deleted, they still have other backdoors they can use. Usually multiple families of APT1 backdoors are found scattered around a victim network when APT1 has been present for more than a few weeks.

2. Use legitimate vPn credentials

APT actors and hackers in general are always looking for valid credentials in order to impersonate a legitimate user. APT1 was observed using stolen usernames and passwords to log into victim networks' VPNs when the VPNs are only protected by single-factor authentication. From there they are able to access whatever the impersonated users are allowed to access within the network.

3. Log in to web portals

Once armed with stolen credentials, APT1 intruders also attempt to log into web portals that the network offers. This includes not only restricted websites, but also web-based email systems such as Outlook Web Access.

complete the mission

Once APT1 finds files of interest they pack them into password protected RAR archive files before stealing them.

```
@echo off
cd /d c:\windows\tasks
rar.log a XXXXXXXX.rar -v200m "C:\Documents and Settings\Place\My
Documents\XXXXXXXX" -hpsmy123!@#
del *.vbs
del %0
```

FIGURE 19: An APT1 batch script that bundles stolen files into RAR archive files

APT1 attackers will transfer files out of the network using the File Transfer Protocol (FTP) or their existing backdoors.

complete the mission

Once APT1 finds files of interest they pack them into password protected RAR archive files before stealing them.

APT1 attacker nsfer Protocol (FTP) or their e

FIGURE 20: APT1 bundles stolen files into RAR archives before moving data to China

PART IV: More Stuxnet

attack scenario

Industrial control systems (ICS) are operated by a specialised assembly like code on *programmable logic controllers* (PLCs). The PLCs are often programmed from Windows computers, the Field PGs, not connected to the Internet or even the internal network. The industrial control systems themselves are also unlikely to be connected to the Internet.

Once Stuxnet infects a computer within the organisation it begins to spread in search of Field PGs. It first tries to spread to other computers on the LAN through a zero-day vulnerability, a two year old vulnerability, infecting Step 7 projects, and through removable drives.

When Stuxnet finally finds a suitable computer, one that ran Step 7, it then modifies the code on the PLC. These modifications sabotage the system.

While their choice of using self-replication methods may have been necessary to ensure they'd find a suitable Field PG, the authors of Student also caused noticeable collateral damage by infecting machines outside the target organisation.

siemens s7-300 (programmed via step 7)

the centrifuges at natanz

scada and natanz

stuxnet basic schema

attack vector

It was impossible to send the malware directly to the Iranian facility, because, of course, it was not connected to an internet network and there were a lot of protective policies. So the creators of Stuxnet thought that these companies would communicate with power plant workers, maybe with USB devices. That's probably how Stuxnet infected the system.

This form of attack is known as *supply-chain attack vector*, whereby the worm is delivered to the target indirectly through its network of contacts.

three layers of cyber-physical attacks

Figure 1: The three layers of a sophisticated cyber-physical attack

Industrial control systems (ICS) are operated by a specialised assembly like code on *programmable logic controllers* (PLCs). The PLCs are often programmed from Windows computers not connected to the Internet or even the internal network. In addition, the industrial control systems themselves are also unlikely to be connected to the Internet.

the unrecognised double payload of student

Stuxnet contains two strikingly different attack routines:

- a complex attack attempts to over-pressurise centrifuges, and qualifies as a plain nightmare for those who understand industrial control system security
- a smaller and simpler attack that changes the speeds of centrifuge rotors

Figure 2: Synopsis of the two different attacks implemented in Stuxnet. Both use a manipulation of industrial control systems to achieve physical damage, exploiting different physical vulnerabilities of the equipment (centrifuge rotors) that basically lead to the same physical result

overpressure attack (1)

In 2007, an unidentified person submitted a sample of code to a collaborative anti-virus platform that much later turned out to be the first variant of Stuxnet. That code contained a payload for interfering with the *Cascade Protection System* (CPS).

The cyber attack against the CPS infects Siemens S7-417 controllers, a top-of-the-line industrial controller for big automation tasks. In Natanz, it is used to control the valves and pressure sensors of up to six cascades (or 6 x 164 = 984 centrifuges) that share common feed, product, and tails stations.

Immediately after infection the payload of this early Stuxnet variant takes over control completely. Legitimate control logic is executed only as long as the malicious code permits it. In a *man-in-the-middle* scenario, the input and output signals are passed from the electrical peripherals to the legitimate program logic and vice versa by attack the code that has positioned itself “in the middle”.

man-in-the-middle

Original system

Infected system

overpressure attack (2)

The attack: process input signals (sensor values) are recorded for a period of 21s. They are replayed in a constant loop during the attack, and show on SCADA screens in the control room, suggesting normal operation

All isolation valves for the first two and the last two enrichment stages are closed, blocking the product and tails outflow of process gas of each affected cascade. More centrifuges are isolated. The consequence is that operating pressure in the other centrifuges increases as UF6 continues to flow into the centrifuge via the feed, but cannot escape via the product and tails take-offs.

The attack continues until the attackers decide that *enough is enough*, based on monitoring vibration sensors and stop before resulting in simultaneous destruction of hundreds of centrifuges per infected controller. This would blow the cover. The intent of the overpressure attack seems to be to increase rotor stress, thereby causing rotors to break early, but not necessarily during the attack run.

This attackis so over-engineered that the attackers faced the risk that the attack might not work at all, as even the slightest oversight –or any configuration change– would result in zero impact or in a immediately detected program crash.

rotor speed attack (1)

New variant discovered in 2010 was much simpler and much less stealthy than its predecessor.

It attacks a completely different component: the *Centrifuge Drive System* (CDS).

It marks a significant change in attitude: Stuxnet became equipped with the latest and greatest MS Windows exploits and stolen digital certificates as the icing on the cake, allowing the malicious software to pose as legitimate driver software and not be rejected by the OS.

Stuxnet had arrived in big information security

But the new Stuxnet was much easier to identify as malicious software than its predecessor.

rotor speed attack (2)

The new attack operates periodically, about once per month. It works by changing rotor speeds: the easy road to trouble is to over-speed the rotors:

normal operating speed of the IR-1 centrifuge is 63,000 rpm
stuxnet increases that speed to 84,600 rpm for fifteen minutes

A month later, a different attack tactic is added, indicating that the first sequence may have left a lot of centrifuges unaffected: bring all centrifuges in the cascade basically to a full stop (120 rpm), only to speed them up again, taking a total of fifty minutes.

The effect of this procedure is not deterministic but offers a good chance of creating damage. The IR-1 is a supercritical design, meaning that operating speed is above certain critical speeds which cause the rotor to vibrate dangerously. Every time a rotor passes through these critical speeds, also called harmonics, it can break.

Very likely causes multiple rotors to break, leaving Iranian operators scratching their heads for a cause: *to chase a demon in the machine*.

Clear evidence that catastrophic destruction was not intended is the fact that no attempts had been made to disable the Cascade Protection System during the rotor speed attack, which would have been much easier than the delicate and elaborate overpressure attack, and prevented the system to deal with the multiple breakages caused by the rotation speed attack.

analysis (1)

Much has been written about the failure of Stuxnet to destroy a substantial number of centrifuges, but the evidence indicates this this was the attackers' intention. If catastrophic damage was caused by Stuxnet, that would have been by accident rather than by purpose.

The attackers were in a position where they could have broken the victim's neck, but they chose continuous periodical choking instead. Stuxnet is a low-yield weapon with the overall intention to reduce the lifetime of Iran's centrifuges and make their fancy control systems appear beyond their engineers' understanding.

A possible explanation is that Iran had mastered the production of IR-1 centrifuges at industrial scale. The simultaneous destruction of all centrifuges would not have set back the Iranian nuclear program for longer than Stuxnet.

Yet, the low-yield approach drove Iranian engineers crazy in the process, up to the point where they may ultimately end in total frustration about their capabilities to get a stolen plant design from the Seventies to run.

Uncovering Stuxnet was the end to the operation, but not necessarily the end of its utility: it showed cyberpower, a scenario nothing short of a Sputnik moment in American history with reversed role. Stuxnet will not be remembered as a significant blow against the Iranian nuclear program. It will be remembered as the opening act of cyber warfare, especially when viewed in the context of the Duqu and Flame malware

analysis (2)

Stuxnet exemplified a methodology for *cyber-physical attack engineering* which is likely to work again. *Physical vulnerabilities* of course depend on the specific production process, plant and configuration, and cannot be reused. To engineer a new attack, the specific vulnerabilities of the target will have to be studied and identified.

No zero-days in industrial control systems. To attack the ICS no fancy exploit was used, just legitimate features. Stuxnet pioneered ideas that can easily be reused: how to inject malicious code in a DLL; how to takeover control from a program which continues to run; how to disable legitimate code; how to feed control code and SCADA with fake sensor data; how to disable cycle time monitoring; how to compromise sub-controllers; how to blindfold sensors by de-calibration; etc. All ready to be copied.

Indirect infiltration via soft targets:

At the operational level Stuxnet proved how to attach the weak links in the supply chain to get to the strong and super protected targets. Any future followup attack will follow these teachings.

analysis (3)

UNIVERSITY OF Southampton

Do future Stuxnet-scale attacks require a state actor to pull them off?

From a technical perspective, certainly not. Stuxnet did for intelligence gathering, infiltration and testing. An attack to a similarly high-value target is likely to require a similar kind of effort and investment. However, there are plentiful accessible and much easier targets on which the teachings of Stuxnet could be replicated at a small price.

All modern plants operate with standard ICS from very few manufacturers, using similar or identical configurations. Network connectivity is often indicated as the main security problems with ICS, but this —together with the unpatched/ unpatchable flaws in the system— is even bigger.

Also, a simultaneous low-key attack on multiple targets of the same kind can have crippling effects as much as a sophisticated attack against a single high-value target: the scalability of the attack makes up the low value of the individual target.

analysis (4)

UNIVERSITY OF Southampton

Can cyber-security controls block Stuxnet-like attacks?

In principle, cyber-security as a whole could block Stuxnet attacks and more. In practice, this is not likely any time soon. None of the classes of defences we know today would be effective against it. Observe in particular that some of the main vulnerabilities exploited by Stuxnet have not been patched yet: in the ICS world, security is not yet a best-practice item.

A political problem:

Cyber offence is well-funded and organised within military chains of commands such as USCYBERCOMMAND and 61398部队. Yet, the cyber defence of critical national infrastructures is expected to come miraculously by a dispersed, uncoordinated private sector whose primary concern is profit. Things are changing in this respect and national committees for the protection of critical national infrastructures are arising even in those countries where the private sectors owns the national infrastructures.

infection statistics

The following graph shows the number of infected organizations by country based on WAN IP addresses:

stuxnet dossier

to kill a centrifuge

Langner

To Kill a Centrifuge

A Technical Analysis of
What Stuxnet's Creators
Tried to Achieve

Ralph Langner

November 2013