GRESHAM COLLEGE

29 MAY 2018

COMPUTERS AND WARFARE

PROFESSOR MARTYN THOMAS

Introduction

Stuxnet, the attacks on the Ukrainian power grid, and autonomous armed guards are only the beginning. Computers are changing warfare profoundly because military strategy has always been geographically based but there are no borders in cyberspace. This lecture considers the implications for the future of international conflict and of national defence. If preparations for the next war have already started, can we tell who is winning?

Computer systems have been essential to the military for many decades. Computers carry out signal processing for radar and sonar, accurate navigation and timing using GPS signals, targeting for bombs, torpedos, missiles and air defence, interception of signals for intelligence and encryption for secrecy, command, control and communications, flight control of aerodynamically unstable aircraft, control of satellites and drones, signal processing for remote surveillance and much much more. But two developments have had a major impact on military strategy in recent years and may revolutionise warfare: they are offensive cyber and the recognition that cyberspace is a fifth dimension of warfare that is at least as important as the other four: land, sea, air and space.

Warfare strategy has traditionally been geographic. The aim is to defend your own territory and to gain control of your enemy's territory, supply lines or freedom of movement, often by dominating strategic locations, for example the Golan Heights, the Strait of Hormuz, the Suez Canal, the Straits of Gibraltar and the South China Sea. If warfare is "the continuation of policy with other means", as Clausewitz wrote[i] then those "other means" have to be effective or policy will suffer.

Geopolitics often relies far more on projecting power than on using it. Positioning an aircraft carrier just outside an adversary's territorial waters strengthens the diplomat's negotiating hand. Strong nations possess powerful weapons and the means to move them into strategic locations and acquiring and maintaining powerful weapons and the aircraft, ships and submarines that support them costs a great deal of money. So the rich nation states have had a great advantage over smaller, poorer states and lesser adversaries.

The extension of warfare into cyberspace undermines traditional strategies because cyberspace has no geographic borders and because cyber weapons can be very powerful without the costs and delays involved in acquiring aircraft carriers or other major weapons and military platforms. Cyber weapons are also much easier to steal or to copy than the traditional weapons that have provided dominance for major powers. In 2017, Harold T Martin III, a former employee of the National Security Agency's elite Office of Tailored Access Operations (TAO), was accused by the US Justice Department of stealing "irreplaceable classified material on a breath-taking scale"[ii]. The theft is said[iii] to include more than 50 terabytes of data, containing over 75% of the offensive cyber tools developed by the TAO. (Some of these tools were later released on the internet and used by cyber criminals to launch the Wannacry and NotPetya ransomware attacks).

When cyber weapons are used, they are likely to reveal the vulnerability that allowed the attack and the way in which it was carried out, which is likely to make the attack less useful in future (security agencies refer to this as "losing an equity"). The use of cyber weapons has also stimulated copycat developments of offensive cyber capabilities as we shall see later when I describe the Stuxnet attack on the centrifuges that were enriching uranium for the Iranian nuclear programme.

Cyber weapons and the non-geographic nature of cyberspace as a battleground take away much of the advantage that the rich and strong nations traditionally had. How can you project power with your aircraft carrier if your adversary has the ability to disable your critical national infrastructure if you refuse to sail away? Or if you cannot be sure who is actually attacking you? Or if your major weapons platforms and military communications are themselves vulnerable to cyberattack? Warfare in cyberspace has created these problems and more, and governments are faced with difficult decisions if military strategy is to remain effective.

Cyberspace

Cyberspace is the universe of computers, the networks that connect them, the online and offline data that they use and manipulate and the displays, sensors and actuators that enable them to interact with people and with all the systems of the physical world.

Cyberspace exists across, outside and beyond geographic borders. Its structure and topology constantly change as connections are made and unmade and create or remove routes for the flow of information and commands. It is addressable but addresses change and need not have a fixed relationship with physical locations or specific devices. Physical distance is usually irrelevant in cyberspace because information may travel at the speed of light and microseconds rarely matter except for very high-frequency financial trading and some complex military and intelligence operations.

Cyberspace is an information space and a command space. It holds and transmits information that ranges from the trivial to the critical, from videos of piano-playing cats and Donald Trump's tweets to emergency tsunami warnings and military intelligence images. It carries commands that range from "open garage door" and "switch on kettle"[iv] to the control of safety-critical industrial systems and the remote operation of lethal weapons.

Uniquely, cyberspace provides access across borders and through walls, giving direct access to millions of people wherever they are, in their offices, bedrooms and in the street. Ubiquitous social media are the world's instant and most trusted source of news and influence. Unfortunately, as **Jonathan Swift** wrote in *The Examiner*, Nov. 9, 1710: "Falsehood flies, and the truth comes limping after it."[v] (a quote often misquoted and misattributed to Mark Twain, Winston Churchill and to anyone else who the speaker feels might have said it).

Attribution and misattribution

It can take a lot of work to track down the true origin of a quotation and the same is true for a cyberattack. The massive Denial of Service attack on Brian Krebs' website was launched from a botnet of hundreds of thousands of hacked video cameras and DVD players[vi] and identifying these individual devices would be no help in finding the controlling mind behind the attack. Yet the botnet Distributed Denial of Service (DDOS) attack on Brian Krebs was a very simple attack compared with many. See, as one example, the covert surveillance of the Dalai Lama that was analysed by researchers at Cambridge University[vii].

When one country fires a ballistic weapon at another country it may be easy to calculate where the attack came from. Some guided missiles are harder to track but still easy by comparison with cyber weapons, which can travel across encrypted networks such as Tor[viii], then exploit computers that are owned by innocent third parties to launch the attack, which could possibly be triggered months later. If a country is cyber-attacked it could easily take many weeks to establish where the attack originated and end up with very low confidence that the attribution is correct.

An adversary may therefore be much more willing to attack, believing that they are anonymous. They may choose to take part in a dispute between two other parties, relying on misattribution to cause an escalation of the conflict to their own advantage. Small states, terrorists, political activists and criminals may see an opportunity to further their own agendas in this way, further eroding the military advantages that major states have historically maintained.

Battle damage estimation and limitation

In warfare the choice of which weapons to use is very important if one's objective is to maximise the effectiveness of the attack on an important target and to limit the civilian casualties. As one example of the care

that is taken by the UK, a drone strike that is planned to kill a terrorist leader may take many weeks of planning and observation to determine the patterns of life in the village where the leader lives, before choosing a moment when they can be seen to be alone and sufficiently far away from anyone else that a precision weapon can be used to kill them. Even then, the strike will be aborted if someone approaches the target at the last minute.

The power and spread of the effect of a missile is known and controllable within limits. Calculating the effect that a cyber strike will have is difficult, because it requires that the effect will be limited to the target system and that the way in which the failure of the target system would affect wider systems is properly understood. That may be easy if the target is an air defence system and the method of access can only affect that system, but if much harder if the target is part of a civilian infrastructure such as an electricity supply network, or if the access method is malware that spreads from system to system.

Countries that comply with laws that forbid attacks on civilian populations or infrastructure are therefore at a disadvantage when their adversary has no such inhibitions, which reduces further the military advantage that major states have historically enjoyed. It may be that some cyber weapons are like nuclear weapons, in that their role can only be deterrence and then only against an adversary who believes that in extremis the weapons will be used and who regards that as a risk that must be avoided.

A sample of known military or state uses of offensive cyber capabilities

In 2007, a large Distributed Denial of Service (DDoS) attack was launched against the **Estonian** cyberspace, disrupting government ministries, banks, media websites and more. Estonia was and remains one of the leading countries for online Government services, voting and banking, which makes it potentially very vulnerable as a target for cyberattacks. Many of the IP addresses that launched the attack were identified as Russian, leading to speculation that an agency affiliated to the Russian government was the attacker. The Estonian Minister of Foreign Affairs linked the attack to recent diplomatic disputes with Russia over the move of a war memorial in Tallinn and claimed that there was evidence of Russian Government involvement in the attack. Russia denied involvement[ix].

Despite this earlier cyber-attack, **Stuxnet**[x] seems to have been the effective starting gun for the international offensive cyber arms race.

The nuclear site in Natanz in **Iran** contains a set of gas centrifuges that are used to enrich uranium. Uranium is a naturally occurring element that is found with two isotopes in very different concentrations: 99.3% uranium 238 and only 0.70% uranium 235. U235 can be used as a nuclear fuel at concentrations of 3% to 4%. U235 can also be used in an atomic bomb at concentrations of 90% or more[xi]. U235 and U238 cannot be separated from each other chemically because they are chemically identical, so they have to be separated using the physical difference that a U238 atom is around 1% heavier than a U235 atom. This separation is done by converting the uranium to uranium hexafluoride gas UF_6 and passing it through a series of tubes that are rotating at supersonic speeds, spinning the heavier U238 to the outside and very gradually increasing the concentration of the required U235. The separation is slow, so it needs a lot of these centrifuges in series. The Iranian plant contained over 7,000 centrifuges - which is enough to enrich sufficient U235 to the 90% concentration needed to fuel one bomb every 6 months. The USA, Israel and other countries were concerned that the enrichment was intended to produce U235 for nuclear weapons rather than as fuel for civil nuclear reactors.

The rotation speed of the Iranian centrifuges was controlled and monitored by computer systems made by Siemens and these were the target for the Stuxnet cyberattack. The Siemens controllers were not connected to the Internet, so the attack had to find a way to cross the air gap: the chosen approach was to infect the computer systems of five companies in the Iranian supply chain with a Windows worm that carried the Stuxnet payload, hoping that the malware would spread and in due course infect USB drives that would be moved between the infected systems and the Siemens controllers attached to the centrifuges. Perhaps surprisingly, this succeeded and the Stuxnet malware was able to reach the controllers, where it had been designed to cause very slight perturbations in the speed of the centrifuges - not enough to alert the operators to the existence of malware but enough to increase the rate at which the centrifuges failed and had to be replaced.

It appears that the Stuxnet attack had been planned at least as early as 2005. The successful infection occurred in 2009 and was causing increased failure rates by 2010. The worm carrying the Stuxnet infection was discovered and identified in the Summer of 2010, because it had spread across many countries and was causing crashes on some Windows computers that were completely unrelated to the Iranian nuclear programme. Stuxnet was sent to security researchers and analysed; they discovered that the payload showed detailed knowledge of the Siemens controller software and exploited a previously unknown (*zero day*) vulnerability in Windows; it also used legitimate digital signatures to avoid detection[xii].

The sophistication of the attack made it seem certain that it was the work of a state intelligence agency. It is assumed to be the work of a joint US and Israeli team. Discovery of the attack seems to have stimulated the Iranian government to develop their own offensive cyber programme.

The attack on Saudi Aramco

The Saudi Arabian company Saudi Aramco is one of the largest oil companies in the world. In August 2012, an IT technician clicked a link in a malicious email and triggered a massive cyber-attack; many systems crashed, many files were lost, and IT staff unplugged computers from servers in Saudi Aramco datacentres worldwide. Every office had to be physically disconnected from the internet so that the malware could not spread and reinfect systems that were being replaced, which meant that although oil production continued at 9.5 million barrels per day, all the sales, invoicing and administration had to be done on paper and using fax machines[xiii]. In all, 30,000 computers were damaged. After 17 days, Aramco started giving oil away for free in Saudi Arabia. Meanwhile, the company hired a large group of consultants and bought 50,000 new hard drives to rebuild their systems. The systems came back online fully five months later.

The attack was claimed in a post[xiv] signed "Cutting Sword of Justice", that said

> *We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.*
>
> *One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. Its hands are infected with the blood of innocent children and people.*
>
> *In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.*
>
> *This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression.*
>
> *Cutting Sword of Justice*

There has been speculation that the attack was actually instigated by Iran[xv] and that they had developed the offensive cyber capability as a direct consequence of their experience of Stuxnet.

In December 2017 another malware attack on a safety-critical industrial control system was described by security analysts at Fireeye[xvi]. The target again seems to have been Saudi Aramco[xvii] (which was at that time organising an Initial Public Offering of its shares). Iran and Russia are suspected of being behind that attack.

The DDoS attack on six US Banks in September 2012

This DDoS attack was described at the time as "the largest cyberattack in history". It caused some disruption and cost the banks tens of millions of dollars but caused no lasting damage and it was handled by the banks

themselves assisted by consultancies and US government agencies. The attack was claimed by a hacker group affiliated to Islamists, but the US security agencies believed that the real source was Iran. President Obama is said to have considered but rejected a proposal that the USA should hack into the Iranian systems in retaliation[xviii].

Cyberattacks against South Korea in March 2013

South Korea has been reported as suffering several small cyberattacks from North Korea most days. In March 2013, three South Korean TV stations and three major banks were infected with the *DarkSeoul* malware that had been designed not to be detected by major antivirus software. The attack caused some 600m Euro economic damage and damaged 48,000 computers. It is assumed that North Korea was responsible for the attack[xix].

The attack on Sony Pictures in the USA in 2014

Sony had made a film called *The Interview* that caused outrage in North Korea because it involved an assassination attempt on Kim Jong-un. In October 2014 a hacker group calling itself *Guardians of Peace* or #GOP destructively infected many Sony computers and also stole a large amount of confidential data[xx] which they released in tranches on the Internet, demanding that the release of the film should be cancelled. The attack was attributed to North Korea and the US Government responded with some economic sanctions against that country.

The attack on the Ukrainian Power Grid

In December 2015 and again in June 2017 the Ukrainian power grid was cyberattacked. The UK National Cybersecurity Centre said that the GRU Russian military intelligence agency was almost certainly responsible, and the UK Foreign Office directly attributed these attacks to Russia

> *"The UK Government judges that the Russian government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack." Lord Ahmad of Wimbledon, Foreign Office minister*[xxi].

The attack on the NHS

The **Wannacry** ransomware attack that seriously disrupted the NHS in May 2017 seems to have been launched by North Korean actors the Lazarus Group[xxii] according to the Foreign Office. The intended target is believed to have been South Korea[xxiii], but the attack affected 300,000 computers in 150 countries. As the New York Times has reported, over a number of years North Korea has become one of the leading offensive cyber powers in the world[xxiv].

Cyberattacks attributed to China

China has been accused of several cyberattacks, including the hacking of the Dalai Lama that I referred to earlier and many other attacks. Foreign Policy magazine listed ten known attacks as long ago as 2010[xxv] , and there have been many accusations since then including an attack in 2011 on 48 chemical and defence companies[xxvi].

Preparations made to facilitate future attacks

Conventional warfare starts with intelligence gathering to inform the military planning, followed by a phase of *transition to war* during which ships, aircraft and troops are readied for action and moved into position. Cyber warfare is no different: there has to be reconnaissance to establish what systems the enemy is using and how they can best be attacked (ideally, if the intent is for example to disable the enemy's air defences, the aim will be to do so in a controlled way so as to limit unintended effects and damage to civilian infrastructure).

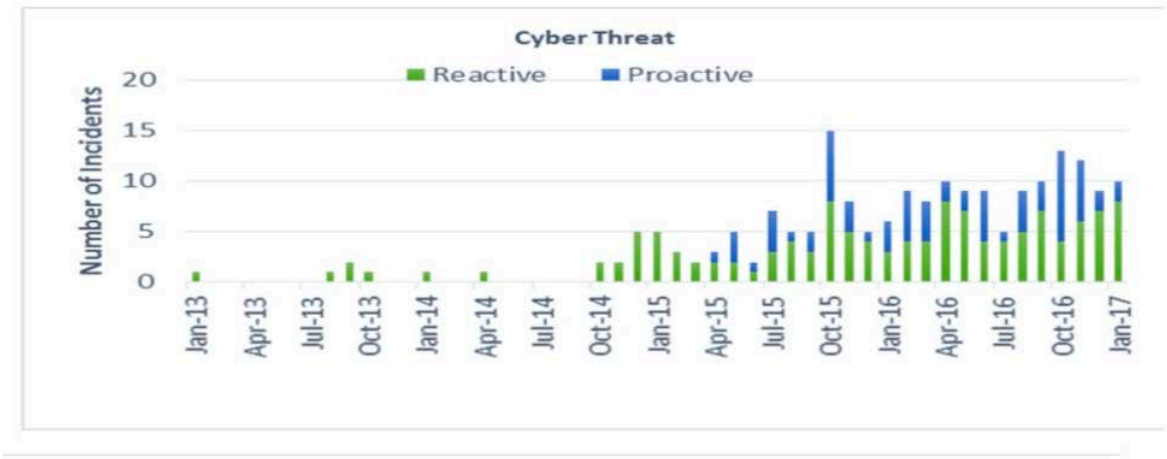
The cyber equivalent of moving aircraft and troops into position is to install malware in the enemy's systems that can be triggered when the order is given to attack.

Such reconnaissance is frequently detected by the staff responsible for monitoring and protecting the UK's Critical National Infrastructure, though the probing will not always (perhaps not even mostly) be part of preparations for an attack — some will be an attempt to steal intellectual property, some will be research by

universities or cybersecurity firms, some will just be mapping of systems by criminals, researchers, businesses and interested amateurs.

As one example, BT Group recently told the UK Parliament Joint Parliament National Security Strategy Committee how often they experience attacks[xxvii], saying that

> *[The figure below] shows the frequency of the most serious threats against BT since January 2013. These threats would have caused disruption to our services had they been successful. We have seen a sharp rise of 1000% in the number of attacks since August 2014, alongside a step change in their complexity and sophistication. In 2017 we saw a rise of 57% in the number of cyber-attacks against BT from the previous year.*



They explained that the lower (green) bars represent attacks against BT whereas the upper (blue) bars represent serious vulnerabilities that they have found themselves. They told the committee that they are at risk from a range of attackers: hackers, criminals, nation states and terrorists. However, the majority of the threats that they see come from organised criminal groups. A major oil and gas company told me recently that they experience "thousands of probes and other attacks every day".

In July 2017 it was reported[xxviii] that a leaked report from the UK National Cybersecurity Centre (NCSC) said that

> *The NCSC is aware of connections from multiple UK IP addresses to infrastructure associated with advanced state-sponsored hostile threat actors, who are known to target the energy and manufacturing sectors … NCSC believes that due to the use of wide-spread targeting by the attacker, a number of Industrial Control System engineering and services organisations are likely to have been compromised.*

The report says that these organisations are part of the supply chain for UK critical national infrastructure, and some are likely to have remote access to critical systems.

Does the world need a non-proliferation treaty for offensive cyber?

An attack on a nation's critical national infrastructure (CNI) could cause widespread injury, death and economic damage. That is precisely why the organisations concerned have been identified as part of the CNI. So should there be a non-proliferation treaty to control the spread of offensive cyber, just as there is for nuclear weapons? It seems that the UK Government does not think so, as the UK-Poland cyber co-operation commitment published 21 December 2017[xxix] says

> *We affirm states' legitimate right to develop both offensive and defensive cyber capabilities and emphasise their obligation to ensure their use is governed in accordance with international law. Acknowledgement of these capabilities does not encourage aggression or contradict our common commitment to maintaining a peaceful ICT environment. Rather, acknowledging the existence of these capabilities fosters the understanding that, just like in the physical domain, Poland and the UK will co-operate to deter, mitigate and attribute malicious cyber-attacks by criminals, state actors and their proxies, including those that seek to interfere in the democratic processes of states.*

Propaganda, persuasion and *psychological operations*

Major Ed Rouse (US Army *retired*) was a specialist in psychological warfare. His website[xxx] describes psychological operations in warfare as follows:

> *Psychological Operations or PSYOP are planned operations to convey selected information and indicators to audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of organizations, groups, and individuals. Used in all aspects of war, it is a weapon whose effectiveness is limited only by the ingenuity of the commander using it. A proven winner in combat and peacetime, PSYOP is one of the oldest weapons in the arsenal of man. It is an important force protector/combat multiplier and a non-lethal weapons system. Psychological Operations (PSYOP) or Psychological Warfare (PSYWAR) is simply learning everything about your target enemy, their beliefs, likes, dislikes, strengths, weaknesses, and vulnerabilities. Once you know what motivates your target, you are ready to begin psychological operations. Psychological operations may be defined broadly as the planned use of communications to influence human attitudes and behavior ... to create in target groups behavior, emotions, and attitudes that support the attainment of national objectives. The form of communication can be as simple as spreading information covertly by word of mouth or through any means of multimedia.*

The rise in social media such as Instagram, Facebook and Twitter has vastly increased the opportunities for psychological operations, whether these are the proven interference in the US Presidential Election and the UK Brexit referendum that I described in my February 2018 lecture *Should We Vote Online?*[xxxi] or "Fake News", or analysis of Facebook updates to discover which soldiers are on which posting so that they can be sent messages threatening that their families will come to harm if they continue to fight.

The recent revelations about the use of Facebook personal data and the analysis of networks of "friends" to target tailored messages to individuals to influence their behaviour is just a small part of the surveillance and analysis of whole populations that is carried out by thousands of companies for their own commercial reasons[xxxii]. This data is often not well protected; it will certainly be exploited in future conflicts.

Autonomous weapons

Autonomous weapons range from the passive (landmines and booby traps, for example) to aircraft and missile defences that can autonomously identify a threat and launch weapons to destroy it. The use of armed robots is increasing and continued growth of the use of artificial intelligence in weaponry is certain; The Economist magazine has referred to autonomous weapons as "a game changer"[xxxiii] that may pose an existential threat.

There is a natural revulsion towards weapons that kill autonomously. The Ottawa Treaty[xxxiv] that seeks to end the use of anti-personnel landmines came into force in 1999; As of January 2018, 164 states are party to the treaty, including Palestine. One country, the Marshall Islands, has signed but not ratified it. There are 34 non-signatories, including major powers such as the United States, Russia, and China. Few countries in the Middle East and South Asia have opted to participate.

Most Western countries have a policy that there should always be a "man in the loop" — by which they mean that a human, male or female, should take the decision about whether to fire a lethal weapon that may kill another human. But this policy is decades behind reality and technology. On 3 July 1988 the USS Vincennes shot down Iran Air flight 655 on a scheduled flight, killing 290 passengers[xxxv]. It seems unlikely that Captain Rogers knowingly shot down a civil plane that was no threat to his ship and that was flying on schedule in a published civil air corridor at 12,000 feet and squawking its identity correctly. It appears that he believed — as the man in the loop — that the target identified by his air defence system was an incoming weapon and that he had to shoot it down to protect his ship and his crew.

As weapons get faster and harder to detect, is it feasible that a human will overrule a future automated system that has identified an imminent threat to that human and their colleagues? Can this doctrine really be enforced when the consequences of firing at a non-existent threat will always be so much less than the consequences of **failing** to fire at a **real** threat? "Man in the loop" is a policy to shift the blame, not to protect life.

The campaign to ban lethal autonomous weapons[xxxvi] has made a powerful campaigning video *slaughterbots*[xxxvii] and they have given permission for part of it to be included in this lecture. So far as I know this weapon has not been built, though the technology to build it exists.

Cybersecurity and the National Defence

Defending military systems is hard because supply chains are long and international, software updates have to be frequent, and almost all the critical software can only be tested and not analysed to assure against critical vulnerabilities because of the way it has been built.

Defending CNI is much harder than defending military systems because most of the UK CNI is owned and operated by private sector organisations that will take their own decisions about the appropriate levels of investment in cybersecurity (and because almost all the critical software can only be tested and not analysed to assure against critical vulnerabilities because of the way it has been built). Defending the thousands of important systems that are outside the formal definition of CNI is currently impossible and not attempted seriously. The UK's industrial strategy encourages inward investment - and ownership of critical infrastructure - by companies headquartered in countries that may become adversaries.

For as long as digital systems continue to be built without the use of strong software engineering, most software will remain vulnerable to cyberattack and the absence of borders in cyberspace will mean that effective national defence cannot be achieved.

Conclusions

The capabilities of computer-based technology and the dependence of society on digital systems are both growing rapidly every year. As I have explained in earlier lectures, almost all software contains a lot of bugs because most software has not been developed using state-of-the-science software engineering[xxxviii]. These bugs - and the carelessness of humans - make most software vulnerable to cyberattack[xxxix].

Offensive Cyber changes the assumptions that underpin almost every aspect of military strategy. There are no borders or geographic constraints. It is very difficult to know who is attacking you or whether or not your key defences have already been penetrated and compromised. The advantages that major powers have historically enjoyed are much weakened, so that a minor adversary may have the power to cause major damage.

Preparation for the next war has already started. Who has control of the major sources of news and influence? Can we tell how vulnerable our hospitals, refineries, food distribution, water and electricity are? What malware is already in place, ready to be triggered? Are we sure that the next war has not already started? If it has, who is winning?

References

[i] https://thediplomat.com/2014/11/everything-you-know-about-clausewitz-is-wrong/

[ii] https://www.washingtonpost.com/world/national-security/prosecutors-to-seek-indictment-against-former-nsa-contractor-as-early-as-this-week/2017/02/06/362a22ca-ec83-11e6-9662-6eedf1627882_story.html

[iii] https://arstechnica.com/tech-policy/2017/02/former-nsa-contractor-may-have-stolen-75-of-taos-elite-hacking-tools/

[iv] see, for instance https://www.gresham.ac.uk/lectures-and-events/the-internet-of-things

[v] http://www.politifact.com/punditfact/statements/2017/oct/09/colin-kaepernick/nfls-colin-kaepernick-incorrectly-credits-winston-/

[vi] https://www.theregister.co.uk/2016/09/26/brian_krebs_site_ddos_was_powered_by_hacked_internet_of_things_botnet/

[vii] *The snooping dragon: social-malware surveillance of the Tibetan movement* Shishir Nagaraja and Ross Anderson, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf

[viii] https://www.torproject.org/

[ix] https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf page 2

[x] For much more detail than I can accommodate in these lecture notes, see https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[xi] http://www.radioactivity.eu.com/site/pages/Uranium_238_235.htm

[xii] https://www.vanityfair.com/news/2011/03/stuxnet-201104

[xiii] http://money.cnn.com/2015/08/05/technology/aramco-hack/

[xiv] https://pastebin.com/HqAgaQRj

[xv] https://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272

[xvi] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[xvii] http://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/

[xviii] https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf page 4.

[xix] https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf page 6

[xx] https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained

[xxi] https://www.telegraph.co.uk/news/2018/02/15/russia-behind-malicious-cyber-attack-ukraine-foreign-office/

[xxii] https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks

[xxiii] https://publications.parliament.uk/pa/cm201719/cmselect/cmdfence/327/32707.htm

[xxiv] https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

[xxv] http://foreignpolicy.com/2010/01/22/the-top-10-chinese-cyber-attacks-that-we-know-of/

[xxvi] https://www.reuters.com/article/us-cyberattack-chemicals/new-cyber-attack-targets-chemical-firms-symantec-idUSTRE79U4K920111031

[xxvii] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-critical-national-infrastructure/written/77350.pdf

[xxviii] https://motherboard.vice.com/en_us/article/9kwg4a/gchq-says-hackers-have-likely-compromised-uk-energy-sector-targets

[xxix] https://www.gov.uk/government/publications/uk-poland-cyber-co-operation-commitment-joint-statement/uk-poland-cyber-co-operation-commitment

[xxx] http://www.psywarrior.com/psyhist.html

[xxxi] https://www.gresham.ac.uk/lectures-and-events/should-we-vote-online

[xxxii] https://www.gresham.ac.uk/lectures-and-events/are-you-customer-or-the-product

[xxxiii] https://www.economist.com/news/special-report/21735472-ai-empowered-robots-pose-entirely-new-dangers-possibly-existential-kind-autonomous

[xxxiv] https://www.armscontrol.org/factsheets/ottawa

[xxxv] https://www.foreignpolicyjournal.com/2017/07/03/the-forgotten-us-shootdown-of-iranian-airliner-flight-655%C2%AD/

[xxxvi] http://autonomousweapons.org/

[xxxvii] https://www.youtube.com/watch?v=HipTO_7mUOw

[xxxviii] https://www.gresham.ac.uk/lectures-and-events/making-software-correct-by-construction

[xxxix] https://www.gresham.ac.uk/lectures-and-events/cybersecurity