Cyberwar

Cyberwar: A guide to the frightening future of online conflict[1]

Updated: With the arrival of cyberwarfare, every device had become a battleground. Here's everything you need to know.

By Steve Ranger 20170829

What is cyberwar?

At its core, cyberwarfare is the use of digital attacks by one country or nation to disrupt the computer systems of another with the aim of create significant damage, death or destruction.

[1] Source: http://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict

What does cyberwarfare look like?

Cyberwar is still an emerging concept, but many experts are concerned that it is likely to be a significant component of any future conflicts. As well as troops using conventional weapons like guns and missiles, future wars will also be fought by hackers using computer code to attack an enemy's infrastructure.

Governments and intelligence agencies worry that digital attacks against vital infrastructure -- like banking systems or power grids -- will give attackers a way of bypassing a country's traditional defences.

And unlike standard military attacks, a cyberattack can be launched instantaneously from any distance, with little obvious evidence in the build-up, and it is often extremely hard to trace such an attack back to its originators. Modern economies, underpinned by computer networks that run everything from sanitation to food distribution and communications, are particularly vulnerable to such attacks, especially as these systems are in the main poorly designed and protected.

The head of the US National Security Agency (NSA) Admiral Michael Rogers said his worst case cyberattack scenario would involve "outright destructive attacks", focused on some aspects of critical US infrastructure and coupled with data manipulation "on a massive scale". Shutting down the power supply or scrambling bank records could easily do major damage to any economy. And some experts warn it's a case of when, not if.

What is the definition of cyberwarfare?

Whether an attack should be considered to be an act of cyberwarfare depends on a number of factors. These can include the identity of the attacker, what they are doing, how they do it -- and how much damage they inflict.

Like other forms of war, cyberwarfare is usually defined as a conflict between states, not individuals. Many countries are now building up military cyberwarfare capabilities, both to defend against other nations and also to attack if necessary.

Attacks by individual hackers, or even groups of hackers, would not usually be considered to be cyberwarfare, unless they were being aided and directed by a state.

For example, cyber-crooks who crash a bank's computer systems while trying to steal money would not be considered to be perpetrating an act of cyberwarfare, even if they came from a rival nation. But state-backed hackers doing the same thing to destabilise a rival state's economy might well be considered so.

The nature and scale of the targets attacked is another indicator: defacing a company website is unlikely to be considered an act of cyberwarfare, whereas disabling the missile defence system at an airbase would certainly come close. And the weapons used are important too: cyberwar refers to digital attacks on computer systems: firing a missile at a data center would not be considered cyberwarfare. Similarly using hackers to spy or even to steal data - cyberespionage - would not in itself be considered an act of cyberwarfare but might be one of the tools used.

Cyberwarfare and the use of force

How these factors combine matters because they can help determine what kind of response a country can make to a cyberattack.

There is one key definition of cyberwarfare, which is a digital attack that is so serious it can be seen as the equivalent of a physical attack.

To reach this threshold, an attack on computer systems would have to lead to significant destruction or disruption, even loss of life. This is a significant threshold because under international law states are permitted to use force to defend themselves against an armed attack.

It follows then that, if a country were hit by a cyberattack of significant scale, they would be within their rights to strike back using their standard military arsenal: to respond to hacking with missile strikes. So far this has never happened -- indeed it's not entirely clear if any attack has ever reached that threshold.

That doesn't mean that attacks which fail to reach that level are irrelevant or should be ignored: it just means that the country under attack can't justify resorting to military force to defend itself. There are plenty of other ways of responding to a cyberattack, from sanctions and expelling diplomats, to responding in kind, although calibrating the right response to an attack is often hard.

What is the Tallinn Manual?

One reason that definitions of cyberwarfare have been blurred is that there is no international law that covers cyberwar, which is what really matters here, because it is such a new concept. That doesn't mean that cyberwarfare isn't covered by the law, it's just that the relevant law is piecemeal, scattered, and often open to interpretation.

This lack of legal framework has resulted in a grey area: in the past some states have used the opportunity to test out cyberwar techniques in the knowledge that other states would be uncertain about how they could react under international law.

More recently that grey area has begun to shrink. A group of law scholars has spent years working to explain how international law can be applied to digital warfare. This work has formed the basis of the Tallinn Manual, a textbook prepared by the group and backed by the NATO-affiliated Cooperative Cyber Defence Centre of Excellence

(CCDCoE) based in the Estonian capital of Tallinn, from which the manual takes its name.

The first version of the manual looked at the rare but most serious cyberattacks, which rose to the level of the use of force; the second edition released earlier this year looked at the legal framework around cyberattacks, which do not reach the threshold of the use of force, but which take place on a daily basis.

Aimed at legal advisers to governments, military, and intelligence agencies, the Tallinn Manual sets out when an attack is a violation of international law in cyberspace, and when and how states can respond to such assaults.

The manual consists of a set of guidelines -- 154 rules -- which set out how the lawyers think international law can be applied to cyberwarfare, covering everything from the use of cyber-mercenaries to the targeting of medical units' computer systems.

The idea is that by making the law around cyberwarfare clearer, there is less risk of an attack escalating, because escalation often occurs when the rules are not clear and leaders overreact.

Which countries are preparing for cyberwar?

According to US intelligence chiefs, more than 30 countries are developing offensive cyberattack capabilities, although most of these government hacking programmes are shrouded in secrecy.

The US intelligence briefing lists Russia, China, Iran, and North Korea as the major "cyber threat actors" to worry about. Russia has a " highly advanced offensive cyber program" and has "conducted damaging and/or disruptive cyber-attacks including attacks on critical infrastructure networks", it warns.

China has also "selectively used cyber attacks against foreign targets" and continues to "integrate and streamline its cyber operations and capabilities", said the report, which also said Iran has already used its cyber capabilities directly against the US with a distributed denial of service attacks targeting the US financial sector in 2012-3. The report also notes that when it comes to North Korea: "Pyongyang remains capable of launching disruptive or destructive cyber attacks to support its political objectives."

US cyberwarfare capabilities

However, it's likely that the US has the most significant cyberdefence and cyberattack capabilities. Speaking last year, President Obama said: "we're moving into a new era

Admiral Michael Rogers, director of the US National Security Agency and head of US Cyber Command Image: Siim Teder/Estonian Defence Forces here, where a number of countries have significant capacities. And frankly we've got more capacity than anybody, both offensively and defensively."

Much of this capability comes from US Cyber Command, lead by Admiral Rogers who also leads the NSA, which has a dual mission: to protect US Department of Defence networks but also to 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 is made up of a number of what it calls Cyber Mission Force teams.

The Cyber National Mission Force teams defend the US by monitoring adversary activity, blocking attacks, and manoeuvring to defeat them.

Cyber Combat Mission Force teams conduct military cyber operations to support military commanders, while the Cyber Protection Force teams defend the Department of Defense information networks.

By the end of fiscal year 2018, the goal is for the force to grow to nearly 6,200 and for all 133 teams to be fully operational. The US is believed to have used various forms of cyber weapons against the Iranian nuclear programme, the North Korean missile tests and the so-called Islamic State, with mixed results.

Reflecting the increased priority the US is putting on cyberwarfare capabilities in August 2017 President Donald Trump upgraded Cyber Command to the status of a Unified Combatant Command, which puts on the same level as groups such as the US Pacific Command and US Central Command. At the same time the Department of Defense said it was also considering separating Cyber Command from the NSA: Admiral Rogers currently heads both organisations and they share staff and resources. Other US agencies like the CIA and NSA have cyberespionage capabilities and have in the past been involved with building cyberweapons - such as the famous Stuxnet worm (see below).

The UK has also publicly stated that is working on cyberdefence and offence projects, and has vowed to strike back if attacked in this manner.

What do cyberweapons look like?

The tools of cyberwarfare can vary from the incredibly sophisticated to the utterly basic. It depends on the effect the attacker is trying to create. Many are part of the standard hacker toolkit, and a series of different tools could be used in concert as part of a cyberattack. For example, a Distributed Denial of Service attack was at the core of the attacks on Estonia in 2007.

Ransomware, which has been a constant source of trouble for businesses and consumers may also have been used not just to raise money but also to cause chaos. There is some evidence to suggest that the recent Petya ransomware attack which originated in Ukraine but rapidly spread across the world may have looked like ransomware but was being deployed to effectively destroy data by encrypting it with no possibility of unlocking it.

Other standard hacker techniques are likely to form part of a cyberattack; phishing emails to trick users into handing over passwords or other data which can allow attackers further access to networks, for example. Malware and viruses could form part of an attack like the Shamoon virus, which wiped the hard drives of 30,000 PCs at Saudi Aramco in 2012.

According to the Washington Post, after revelations about Russian meddling in the run up to the 2016 US Presidential elections, President Obama authorised the planting cyber-weapons in Russia's infrastructure. "The implants were developed by the NSA and designed so that they could be triggered remotely as part of retaliatory cyber-strike in the face of Russian aggression, whether an attack on a power grid or interference in a future presidential race," the report said.

Cyberwarfare and zero-day attack stockpiles

Zero-day vulnerabilities are bugs or flaws in code which can give attackers access to or control over systems, but which have not yet been discovered and fixed by software companies. These flaws are particularly prized because there will likely be no way to stop hackers exploiting them. There is a thriving trade in zero-day exploits that allow hackers to sidestep security: very handy for nations looking to build unstoppable cyber weapons. It is believed that many nations have stock piles of zero day exploits to use for either cyber espionage or as part of elaborate cyber weapons. Zero day exploits formed a key part of the Stuxnet cyberweapon (see below).

One issue with cyberweapons, particularly those using zero-day exploits is that -- unlike a conventional bomb or missile -- a cyberweapon can be analysed and even potentially repurposed and re-used by the country or group it was used against.

One good example of this is shown by the WannaCry ransomware attack which caused chaos in May 2017. The ransomware proved so virulent because it was supercharged with a zero-day vulnerability which had been stockpiled by the NSA, presumably to use in cyberespionage. But the tool was somehow acquired by the Shadow Brokers hacking group which then leaked it online, after which the ransomware writers incorporated it into their software, making it vastly more powerful.

This risk of unexpected consequences mean that cyberweapons and tools have to be handled - and deployed - with great care. There is also the further risk that thanks to the hyper-connected world we live in that these weapons can spread much also cause much greater chaos than planned, which is what may have happened in the case of the Ukrainian Petya ransomware attack.

What is Stuxnet?

Stuxnet is a computer worm that targets industrial control systems, but is most famous for most likely being the first genuine cyber-weapon, in that it was designed to inflict physical damage.

It was developed by the US and Israel (although they have never confirmed this) to target the Iranian nuclear programme. The worm, first spotted in 2010, targeted specific Siemens industrial control systems, and seemed to be targeting the systems controlling the centrifuges in the Iranian uranium enrichment project -- apparently damaging 1,000 of these centrifuges and delaying the project, although the overall impact on the programme is not clear.

Stuxnet was a complicated worm, using four different zero-day exploits and likely took millions of dollars of research and months or years of work to create.

Is cyberwarfare escalation a concern?

There is a definite risk that we are at the early stages of a cyberwar arms race: as countries realise that having a cyberwarfare strategy is necessary they will increase spending and start to stockpile weapons, just like any other arms race. That means there could be more nations stockpiling zero-day attacks, which means more holes in software not being patched, which makes us all less secure. And countries with stockpiles of cyberweapons may mean cyberconflicts are able to escalate quicker. One of the big problems is that these programmes tend to be developed in secret with very little oversight and accountability and with mirky rules of engagement.

What are the targets in cyberwar?

Military systems are an obvious target: preventing commanders from communicating with their troops or seeing where the enemy is would give an attacker a major advantage.

However, because most developed economies rely on computerised systems for everything from power to food and transport many governments are very worried that rival states may target critical national infrastructure. Supervisory control and data acquisition (SCADA) systems, or industrial control systems, which run factories, power stations and other industrial processes are a big target, as Stuxnet showed.

These systems can be decades old and were rarely designed with security as a priority, but are increasingly being connected to the internet to make them more efficient or easy to monitor. But this also makes these systems more vulnerable to attack, and security is rarely upgraded because the organisations operating them do not consider themselves to be a target.

A short history of cyberwar

For many people 2007 was when cyberwar went from the theoretical to the actual.

When the government of the eastern European state of Estonia announced plans to move a

Soviet war memorial, it found itself under a furious digital bombardment that knocked banks and government services offline (the attack is generally considered to have been Russian hackers; Russian authorities denied any knowledge). However, the DDoS attacks on Estonia did not create physical damage and, while a significant event, were not considered to have risen to the level of actual cyberwarfare.

Another cyberwarfare milestone was hit the same year, however, when the Idaho National Laboratory proved, via the Aurora Generator Test, that a digital attack could be used to destroy physical objects -- in this case a generator.

The Stuxnet malware attack took place in 2010, which proved that malware could impact the physical world.

Since then there has been a steady stream of stories: in 2013 the NSA said it had stopped a plot by an unnamed nation -- believed to be China -- to attack the BIOS chip in PCs, rendering them unusable. In 2014 there was the attack on Sony Pictures Entertainment, blamed by many on North Korea, which showed that it was not just government systems and data that could be targeted by state-backed hackers.

Perhaps most seriously, just before Christmas in 2015 hackers managed to disrupt the power supply in parts of Ukraine, by using a well-known Trojan called BlackEnergy. In March 2016 seven Iranian hackers were accused of trying to shut down a New York dam in a federal grand jury indictment.

Nations are rapidly building cyberdefence and offence capabilities and NATO in 2014 took the important step of confirming that a cyberattack on one of its members would be enough to allow them to invoke Article 5, the collective defence mechanism at the heart of the alliance. In 2016 it then defined cyberspace as an "operational domain" -- an area in which conflict can occur: the internet had officially become a battlefield.

Cyberwar and the Internet of Things

Big industrial control systems or military networks are often considered the main targets in cyberwarfare but one consequence of the rise of the Internet of Things may be to bring the battlefield into our homes.

"Our adversaries have capabilities to hold at risk US critical infrastructure as well as the broader ecosystem of connected consumer and industrial devices known as the Internet of Things," said a US intelligence community briefing from January 2017. Connected thermostats, cameras, and cookers could all be used either to spy on citizens of another country, or to cause havoc if they were hacked.

How do you defend against cyberwarfare?

The same cybersecurity practices that will protect against everyday hackers and cyber-crooks will provide some protection against state-backed cyberattackers, who use many of the same techniques. That means covering the basics: changing default passwords and making passwords hard to crack, not using the same password for different systems, making sure that all systems are patched and up-to-date (including the use of antivirus software), ensuring that systems are only connected to the internet if necessary and making sure that essential data is backed up securely. This may be enough to stop some attackers or at least give them enough extra work to do that they switch to an easier target.

Recognising that your organisation can be a target is an important step: even if your organisation is not an obvious target for hackers motivated by greed (who would hack a sewage works for money?) you may be a priority for hackers looking to create chaos.

However, for particularly high-value targets this is unlikely to be enough: these attacks are called 'advanced and persistent'. In this case it may be hard to stop them at the boundary and additional cybersecurity investments will be needed: strong encryption, multi-factor authentication and advanced network monitoring. It may well be that you cannot stop them penetrating your network, but you may be able to stop them doing any damage.

What is cyberespionage?

Closely related but separate to cyberwarfare is cyberespionage, whereby hackers infiltrate computer systems and networks to steal data and often intellectual property. There have been plenty of examples of this in recent years: for example the hack on the US Office of Personnel Management, which saw the records of 21 million US citizens stolen, including five million sets of fingerprints, was most likely carried out by Chinese state-backed hackers.

Perhaps even more infamous: the hacking attacks in the run up to the 2016 US

Presidential elections and the theft of emails from the Democratic National Committee: US intelligence said that Russia was behind the attacks. The aim of cyberespionage is to steal, not to do damage, but it's arguable that such attacks can also have a bigger impact. Law scholars are, for example, split on whether the hacks on the DNC and the subsequent leaking of the emails could be illegal under international law.

Some argue that it mounts up to meddling in the affairs of another state and therefore some kind of response, such as hacking back, would have been justified; others argue that it was just below the threshold required. As such the line between cyberwarfare and cyberespionage is a blurred one: certainly the behaviour necessary is similar for both -- sneaking into networks, looking for flaws in software -- but only the outcome is different; stealing rather than destroying. For defenders it's especially hard to tell the difference between an enemy probing a network looking for flaws to exploit and an enemy probing a network to find secrets.

"Infiltrations in US critical infrastructure -- when viewed in the light of incidents like these -- can look like preparations for future attacks that could be intended to harm Americans, or at least to deter the United States and other countries from protecting and defending our vital interests," NSA chief Rogers said in testimony to the US Senate.

Cyberwarfare and information warfare

Closely related to cyberwarfare is the concept of information warfare; that is, the use of disinformation and propaganda in order to influence others -- like the citizens of another state. This disinformation might use documents stolen by hackers and published -- either complete or modified by the attackers to suit their purpose. It may also see the use of social media (and broader media) to share incorrect stories. While Western strategists tend to see cyberwarfare and hybrid information warfare as separate entities, some analysts say that Chinese and Russia military theorists see the two as closely linked. Indeed it is possible that Western military strategists have been planning for the wrong type of cyberwar.

What are cyber wargames?

One of ways countries are preparing to defend against cyberwarfare is with giant cyberdefence wargames, which pit a 'red team' of attackers against a 'blue team' of defenders.

Some of biggest international cyberdefence exercises, like the NATO-backed Locked Shields event, can see as many as 900 cybersecurity experts sharpening their skills. In Locked Shields the defending teams have to protect small, fictional, NATO member state Berylia from mounting cyberattacks by rival nation Crimsonia.

From malware to cyber-spies, the 15 biggest threats online, ranked[2]

When it comes to cybersecurity, what should you really be worried about?

By Steve Ranger 20170222

Europe's computer security agency has set out a list of the top threats in the online world, warning that hacking for profit is one of the biggest trends.

"Undoubtedly, optimization of cyber-crime turnover was THE trend observed in 2016. And, as with many of the negative aspects in

[2] Source: http://www.zdnet.com/article/from-malware-to-cyber-spies-the-15-biggest-threats-online-ranked/

cyber-space, this trend is here to stay. The development and optimization of badware towards profit will remain the main parameter for attack methods, tools and tactics," warned the report from the European Union Agency for Network and Information Security (ENISA).

It said criminals had been using unsecured Internet of Things (IoT) devices to launch giant distributed denial of service (DDoS) attacks, and have launched extortion attacks against commercial organisations that have "achieved very high levels of ransom and high rates of paying victims", and demonstrated the ability to affect the outcome of democratic processes like the US presidential elections.

Executive director of ENISA Udo Helmbrecht said: "As we speak, the cyber-threat landscape is receiving significant high-level attention: it is on the agenda of politicians in the biggest industrial countries. This is a direct consequence of 'cyber' becoming mainstream, in affecting people's opinions and influencing the political environment of modern societies."

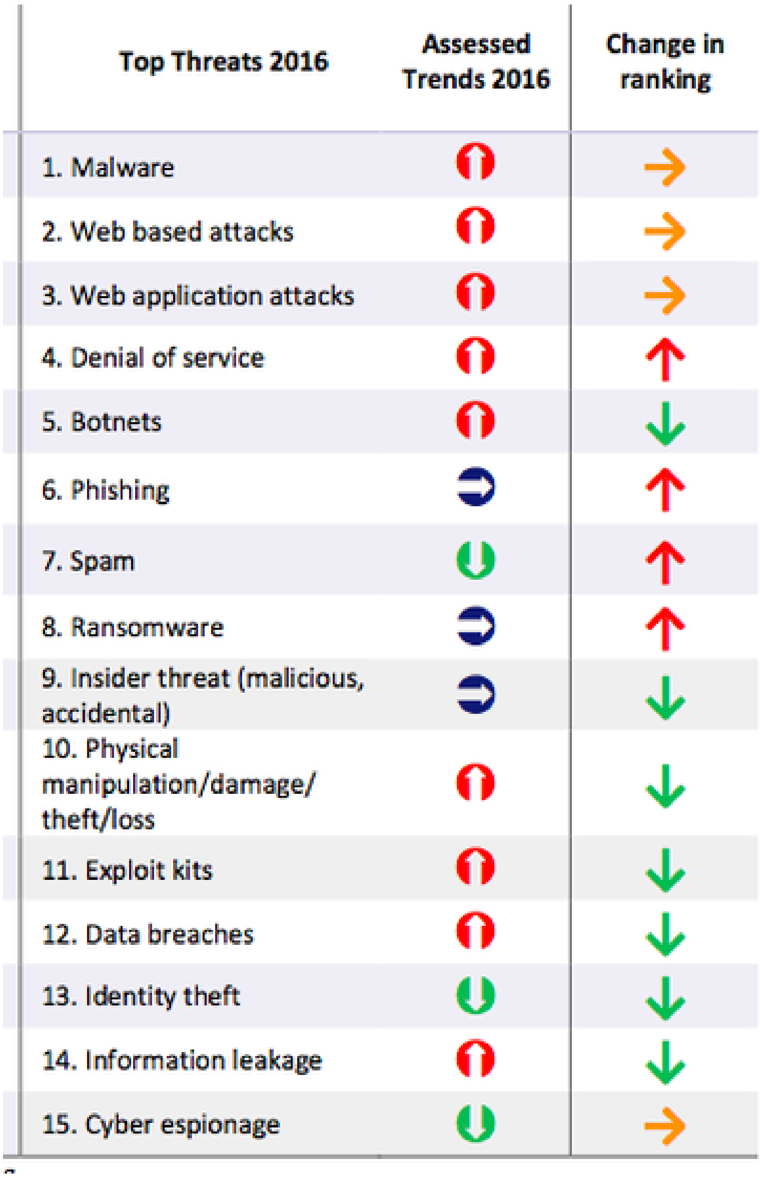
Malware tops ENISA's lists, with over 600 million samples identified per quarter, and mobile malware, ransomware, and information stealers the main areas of criminal malware innovation.

"Equally impressive was the fact that state-sponsored threat actors have launched malware that has had high efficiency by exploiting quite a few zero-day vulnerabilities," the report said.

It noted that the average lifespan of malware hashes -- the unique identification of a malware variant used by malware detection tools -- has shrunk so much that a specific malware variant might exist for just one hour.

"This is indicative of the speed of malware mutation in order to evade detection on the one hand, and one of the reasons for gaps in end-point protection measures (i.e. anti-virus software)," it said.

The report also blamed the availability of 'malware-as-a-service' offerings, which allow users to rent the infrastructure for a few thousand dollars per month to launch, for example, ransomware attacks with $100,000 monthly revenues.



Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	↑	→
2. Web based attacks	↑	→
3. Web application attacks	↑	→
4. Denial of service	↑	↑
5. Botnets	↑	↓
6. Phishing	→	↑
7. Spam	↓	↑
8. Ransomware	→	↑
9. Insider threat (malicious, accidental)	→	↓
10. Physical manipulation/damage/ theft/loss	↑	↓
11. Exploit kits	↑	↓
12. Data breaches	↑	↓
13. Identity theft	↓	↓
14. Information leakage	↑	↓
15. Cyber espionage	↓	→

The digital threat landscape according to ENISA.Image: ENISA

The report said that DDoS attacks -- once used by activists to disrupt corporate websites -- are now being used for extortion attempts, part of the trend toward monetising hacking. Similarly, the report noted that phishing has successfully reached the executive level: CEO fraud is now causing significant losses to companies.

And while it may be a surprise that, following the controversy around the US presidential election, ENISA ranked cyber-espionage at the bottom of its list, it noted: "Known/confirmed cases are the top of the iceberg. This is because espionage campaigns are difficult to identify. And once identified are difficult/costly to analyse. It is believed that cyber-espionage is the motive of much more undetected campaigns. To this extent, the assessed descending trend of this threat may not be fully valid. Secondly, cyber-espionage is much targeted: it uses the same methods as cyber-crime, but it possesses intelligence allowing it to lure victims much more efficiently."

US intelligence: 30 countries building cyber attack capabilities[3]

Officials say Russia has "highly advanced" offensive cyber program, and that only its 'senior-most' officials could have authorized election-focused data thefts.

By Steve Ranger | 20170105

US director of national intelligence James Clapper giving testimony in Congress previously. (Image: C-SPAN/file photo)

More than 30 countries are developing offensive cyber attack capabilities, according to US intelligence chiefs.

[3] http://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/

They warn that cyber attacks against critical infrastructure and information networks will give attackers a means of bypassing traditional defence measures.

The warning came in a joint statement by US director of National Security James Clapper, undersecretary of defense for intelligence Marcel Lettre, and NSA and US Cyber Command director Admiral Mike Rogers, at a hearing on foreign cyber threats by the Senate Armed Services Committee.

"Protecting critical infrastructure such as crucial energy, financial, manufacturing, transportation, communication, and health systems, will become an increasingly complex national security challenge," the written statement noted.

It also warned that nations equipped with similar offensive cyber capabilities could be prone to preemptive attack and rapid escalation in a future crisis, "because both sides would have an incentive to strike first".

The committee was meeting in the aftermath of what its chairman Senator John McCain called an "unprecedented attack on our democracy", referring to the hacking attacks during the recent Presidential election, which have been blamed by US intelligence on Russia.

President-elect Donald Trump has cast doubt on whether Russia was behind the attacks.

However, the statement from the intelligence chiefs said Russia is a "full-scope cyber actor" and one that "poses a major threat to US government, military, diplomatic, commercial, and critical infrastructure and key resource networks because of its highly advanced offensive cyber program and sophisticated tactics, techniques, and procedures".

It said Russian cyber operations had targeted government organizations, criticial infrastructure, think tanks, universities, political organizations and corporations, often using spearphishing campaigns.

"We asses that only Russia's senior-most officials could have authorized the recent election-focused data thefts and disclosures, based on the scope and sensitivity of the targets," the statement continued.

"Every American should be alarmed by Russia's attack on our nation," McCain said. But the recent Russian attacks are one part of a bigger cyber problem he added, pointing to other digital espionage and cyber attacks by hackers aligned with China and North Korea.

"What seems clear is our adversaries have reached a common conclusion that the reward for attacking American cyberspace outweighs the risk. For years cyber attacks on our nation have been met with indecision and inaction. Our nation has no policy and thus no strategy for cyber deterrence. Unless we demonstrate that the costs of attacking the United States outweigh the perceived benefits these cyber attacks will only grow," he warned.

Certainly Russia was not the only digital threat the intelligence chiefs identified.

China continues to conduct cyber espionage against the US government and companies, albeit at lower levels than previously, they said. "Beijing has also selectively used cyber attacks against foreign targets that it probably believes threaten Chinese domestic stability or regime legitimacy." They also listed Iran as using cyber espionage, propoganda and attacks, and said North Korea remains capable of "launching disruptive or destructive cyber attacks to support its political objectives".

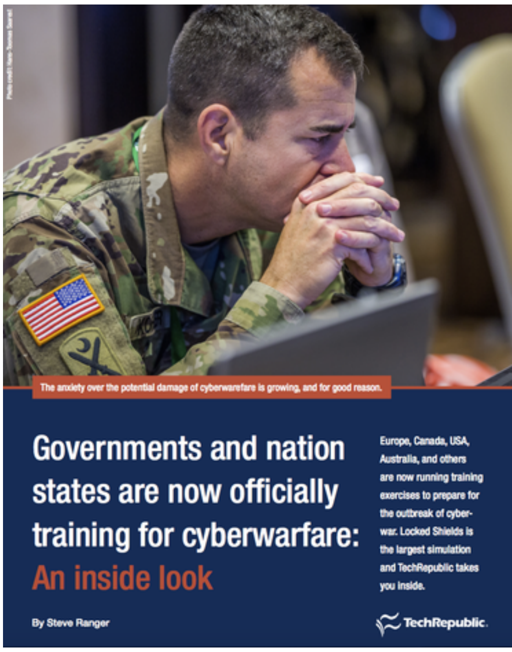
And the risk isn't likely to decline, either: "Over the next five years, technological change will only accelerate the intersection of cyber and physical devices, creating new risks," they said.

Governments and nation states are now officially training for cyberwarfare: An inside look[4]

Steve Ranger Date?

Berylia is under attack. Again.

The island nation, located somewhere in the cold waters of the Atlantic Ocean, relies on its state-of-the-art drone industry for a large part of its income. But recently its drone research labs have come under



The anxiety over the potential damage of cyberwarfare is growing, and for good reason.

Governments and nation states are now officially training for cyberwarfare: An inside look

Europe, Canada, USA, Australia, and others are now running training exercises to prepare for the outbreak of cyber-war. Locked Shields is the largest simulation and TechRepublic takes you inside.

By Steve Ranger

TechRepublic.

TechRepublic cover

[4] Source: http://www.techrepublic.com/article/governments-and-nation-states-are-now-officially-training-for-cyberwarfare-an-inside-look/

cyber attack from unknown assailants, forcing Berylia to deploy rapid-reaction teams of security experts to its labs, under orders to find out what's happening, and to stop the attacks as quickly as possible.

Over two hectic days, the teams will have to battle against mounting attacks on their systems, hijacking of their drones, and questions from a sometimes hostile press.

And it's not the first time Berylia has come under attack: strangely these cyber onslaughts happen every year at around the same time. And these incursions won't be the last time the country comes under attack either, because the fictional drone-building country is the setting for the NATO annual cyber defence wargame, Locked Shields.

The exercise is run from Estonia by NATO's cyberwarfare think tank, the Cooperative Cyber Defence Centre of Excellence (CCD COE). The annual event, which has been running since 2010, aims to train the security experts who protect national IT systems on a daily basis. While the exact scenario changes every year, the setting—the embattled Berylia—remains the same, and arch-rival Crimsonia often makes an appearance too.

Berylia might be a fictional state, but Estonia itself has first hand experience of these sort of digital attacks: back in 2007 its banks and government systems suffered weeks of disruption from hackers after Estonian authorities proposed moving a Soviet war memorial. Russia denied any involvement in the attacks, but the incident accelerated plans for the formation of the NATO's cyber think tank, located in the Estonian capital, Tallinn.

This year Locked Shields saw more than 1,700 attack carried out against 1,500 virtualised systems being protected by 20 teams, which separately had to defend online services and industrial control systems against real malware and digital attacks.

The wargame pits 20 'blue team' sets of defenders from NATO's member states, against a 'red team' of attackers which attempt to disrupt their networks. A separate 'white team' of experts runs the game systems. In total, the exercise involves around 550 people across 26 nationalities, 250 of which are the core planning team in Tallinn, where the main action takes place over a two-day period.

It's not the only big cyber wargame. The US runs its own 'Cyber Guard' event every year, which this year saw around 1,000 players from various government agencies. Those taking part included the UK, Canada, and Australia, all dealing with a fictional attack on an oil refinery, power grids, and ports, while the Bank of England has overseen 'Waking Shark' exercises across the banks in London. However, Locked Shields describes itself as the largest international technical cyber defence exercise.

Berylia
Crimsonia
Revalia

Berylia and Crimsonia are the two fictional countries involved in the Locked Shields simulation.Image: Hans-Toomas Saarest

All the Locked Shields teams get the same mission briefing, and the same set of virtual systems to defend. While the game is run from Estonia by NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE), most teams log-in remotely from their own countries. The teams are playing simultaneously but separately, so it is in some respects 20 games at once, although the teams are allowed to share some information.

In the scenario, the teams are playing as a rapid reaction team that has just been dropped into a drone research lab. That means when the game starts, they don't even know precisely what systems they have to defend, and whether their adversary has already managed to breach any.

Even the technical information they are given about the systems they have been called in to protect is—as it would be in real life—shoddy and possibly incorrect, making it even harder for the teams to prepare their defences.

"We are trying to use hacking scenarios and attack scenarios that are taken from real life, so we are not playing on an abstract simulation, we are actually using the same operating systems that would be encountered in real life," Dr Rain Ottis, Locked Shields 2016 scenario master, said.

"We want to see how they handle themselves as a team in a situation where there's lots of fog of war, where you do not have full visibility of the scenario of the things that are happening to you," he said.

Over the course of the exercise things only get worse. Not only do the teams have to deal with incoming attacks, they also have to deal with getting blamed for attacks coming from their networks. "It is as realistic as we can make it," said Ottis.

The teams of defenders—each of around a dozen people—have to protect around 2,000 machines making up a realistic representation of what a business network would look like. The services the blue teams have to maintain range from websites, email, and online shopping services, to various kinds of industrial control systems.

The aim is to put constant pressure on the defending teams, to test them with the sort of full-scale cyber attack that hardened security professionals would hope to never experience in real life.

"We have absolutely everything in there, we have Windows 7, 8, 10, we have Apple OS X, we brought in most of the Linux versions, so what we want to do is have a wide spectrum of operating systems. Everything you can imagine in a regular office, all the software and hardware, we try to simulate that and show that in some way they can be vulnerable," said Aare Reintam, CCD COE's technical exercise director.

"We want to show them everything you have in the environment can be a target or a jumping point into your internal networks," he said.

That means that everything from smartphones to humble printers could be a target. "We want to express that absolutely everything that you have in the network can be a target, that you have to defend everything. Attackers have to find only one thing to attack," he said.

As such, teams don't just have to protect standard PCs or servers, the Internet of Things is part of the security threat too. In the scenario, the teams are protecting a drone research lab, so one of the challenges they are faced with is keeping control of the command and control system for the drones—and regaining control of the drones if it's lost.

Perhaps one of the more unexpected systems they need to protect is an industrial command and control system. The one that runs the cooling in their own server room. If the teams lose control of that, then their mysterious enemies can turn up the heat, and shut their servers down (to add a little drama to the proceedings when this happens sparks shoot out of the server room simulation board).

The teams respond to the challenges differently, and one tempting option of course when faced with an overwhelming cyberattack is to pull the plug—to protect the systems by taking them offline. But that would be to miss the point: teams must be able to protect the systems while keeping them up and running, even if they have to prioritise.

For Reintam, this is one of the keys to the event: "We are teaching them how to protect our lifestyle. We have to make sure that the lifestyle that we are used to, that you wake up in the morning and you turn on your lights, that you turn on the water and can make yourself a coffee, that you can browse the news with your coffee... you have to pay attention to every aspect of the ecosystem and you have to protect it."

The game wouldn't get very far without the red team, which aims to create that fog of war that surrounds the defending teams. It has around 60 members to "entertain" the defending blue team, said Mehis Hakkaja, head of the red team and CEO of Clarified Security. The red team uses attack methods that are out in the wild to make attacks as realistic as possible, although still ones that can be defended against.

Even though the red team knows most blue team systems and vulnerabilities beforehand and even has pre-planted backdoors, the situation changes rapidly as soon as the exercise starts, he said: some of the attacks are based on cybersecurity basics like missing patches but can rapidly accelerate to attacks on complex industrial control systems.The red team can pretend to be various typical hacker groups—from stealthy 'advanced persistent threat' actors to noisier and apparently less skilled hacktivists—or perhaps both at the same time, depending on the scenario. The game plan changes depending on how well the teams respond. The attackers will attempt to do things like steal documents which are then leaked to the in-game media, but if the teams managed to thwart that heist then the game goes in another direction instead.

Playing through such a variety of attacks and threat actors from various angles allows the red team and organisers to evaluate the blue teams on their ability to notice and respond, whether their initial defensive plan worked, and whether they managed to retain control and a sufficient situational overview.

"Having a good initial defence strategy is good, but ability to adjust it on-the-fly is even more important," Hakkaja said, as it seeing the bigger picture, "because just blocking and blindly trying to apply defences, or only seeing some attack indications only gets you so far."

As well as the technical aspects of the game, the teams are also tested on their understanding of the legal issues involved with protecting against the attacks, how they deal with the press, and how well they report back to their fictional commanders or political leaders.

This battlefield has traded trenches and firearms for desks, monitors, keyboards, and lots of cables.Image: Hans-Toomas Saarest

In the media element of the game, the teams for example have to be able to explain their actions and put across their point of view accurately, even when being questioned by hostile journalists who are trying to trick the teams into saying too much or saying the wrong thing, all of which plays out on the in-game news site. Another element tested is around legal issues. The legal picture around hacking, and cyberwarfare in particular, is often unclear, so the teams have to do everything they can to ensure that they are behaving legally.

For example, the legal framework used during armed conflict is different to those used in standard policing, so working out whether a cyber incident has risen to the level of an armed conflict is a key factor, something that is hard for defenders to work out when many of these attacks are stealthy and anonymous. Malware doesn't wear a uniform or carry a flag.

During the exercise, the legal advisors on the team are tested, often in coordination with the other events in the game: for example, being asked to give military commanders advice on their options when dealing with hacked drones.

"In every military operation the idea is to get the commander the options to chose from, and each of those option need to be assessed by a lawyer to say what legal issues do they raise, is it lawful in the first place, which is the best option from a legal perspective," explains Dr. Heather Harrison Dinniss, head of the Locked

Shields legal team and senior lecturer in International Law at the Swedish Defence University.

It's only in the last few years—with the publication of documents like the Tallinn Manual which looks at how international law applies to cyberwarfare—has the legal framework around cyberwarfare has become clearer.

"The difficulty when you are dealing with cyber, of course, is you don't necessarily know who it is that is launching the attack," Harrison Dinniss said. "Cyber makes that assessment more difficult."

"There's a much greater acceptance now that the law applies," she added, although there are still things that are uncertain: for example, while it's generally agreed that a serious cyber attack could be considered the equivalent of an armed attack, there's less agreement about how to treat less physically destructive attacks.

"There are still interpretation issues, something that's still up in the air is what do we do about data-only attacks," she said. We're talking about ones that don't cause any physical damage but wipe computer systems, like the attack on Saudi Aramco in 2012 which wiped more than 30,000 devices.

"There is still a question of how do we treat that because there is no physical harm. What do you do when they wipe the computers and make them unusable. Is that enough? Is that a use of force? There's still significant disagreement on [that]," she said.

Teams also have to make sure they do the paperwork.

"We do want them to be able to write human-readable reports about what is going on, something they could send to a manager or a government minister—so condense what they know into something that a non-tech expert can understand, because we have seen time and again that this is a weak spot in the cybersecurity community. We like the lingo that we use and it's sometimes why the message gets lost, and we train for that," said scenario master Ottis.

The exercise puts a lot of emphasis on team communication, team leadership, and delegation. So what makes a good cyber defence team?

The best teams tend to have done some preparation by thinking through the skills and tools that they will need. Those teams typically figure out who is taking which role quickly, too, so they don't have to worry about who is looking after which systems when the action begins.

Winning teams try to understand the battlefield, predict what their attackers are going to do next, and try to be ready for it, said Ottis.

"We like to see where you are trying to figure out the battlefield, know yourself, know your adversary, and make your plan based on that," Ottis added. "Figure out where you need sensors, which service require more manual monitoring, and which ones you can leave on the back burner. We are talking about being proactive within the network that you have."

Head of the red team Hakkaja makes a similar point: "To see, understand, and communicate the big picture, not being lost in the small technical pieces, is probably the hardest for techies. Large scale cyber exercises like Locked Shields provide a unique opportunity for blue teams to be in such rapidly evolving situations where they rarely are in their daily job as a team."

However, there's one thing that teams can't do, and that is strike back against their adversaries. "This is a strictly defensive exercise so we want them to defend what they have, we want them we want them to cooperate if it makes sense, we want them to keep communications up with the rest of the world and with their higher command. But we do not want them to go on the offensive because that has very serious legal repercussions," said Ottis.

The team from Slovakia won this year's event at the end of April, closely followed by the NATO Computer Incident Response

Capability (NCIRC) team from NATO and Finland, which won last year. The Slovakia team scored highest in the media challenges of the exercise and Germany came out on top of the forensic game, while NCIRC did the best in providing legal analysis, and the Czech Republic won scenario challenges.

"When under intense pressure, network security professionals have to monitor the environment, consider social, political, and legal consequences as well as keep ahead of the constant technical challenges," said Thomas Svensson, inject master of Locked Shields 2016.

Technical exercise director Reintam said there is huge demand for the exercise, reflecting how many countries in NATO are increasingly worried about cyber defence, especially the Baltic states. Worried about Russian cyber attacks, Estonia has even been discussing backing-up vast amounts of public data, from birth records to property deeds, in a secure location outside of the country.

As such, NATO has been taking cyberwarfare increasingly seriously in recent years, first making it clear that a serious cyber attack could trigger its collective defense clause and more recently defining cyberspace as a an operational domain—that is, a likely battlefield.

However, many members lack the trained staff to recognise or deal with a serious cyber attack on their critical national infrastructure. Events like Locked Shields are aimed at encouraging members to take their digital defences more seriously, and perhaps also to show potential aggressors that NATO takes the threat seriously, too.

Right now, all is quiet again in Berylia. But perhaps for not too much longer.

20170830 Assembled by Wergosum