What is cyberwar? Everything you need to know about the frightening future of digital conflict | ZDNet

Steve Ranger

x

player version	0.42.297
stream type	HLS
playback state	1
duration	407.2874439999993
current time	65.33
buffer length	96.10
average dropped (fps)	0.00
playback framerate (fps)	23.98
switching mode	auto
transition state	complete
start index bitrate (B/s)	-0.00k
current bandwidth (B/s)	46.26M

0:00 / 0:00

What is cyberwar?

Cyberwarfare refers to the use of digital attacks -- like computer viruses and hacking -- by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction. Future wars will see hackers using computer code to attack an enemy's infrastructure, fighting alongside troops using conventional weapons like guns and missiles.

A shadowy world that is still filled with spies, hackers and top secret digital weapons projects, cyberwarfare is an increasingly common -- and dangerous -- feature of international conflicts. But right now the combination of an ongoing cyberwarfare arms race and a lack of clear rules governing online conflict means there is a real risk that incidents could rapidly escalate out of control.

- Cyberwar: What happens when a nation-state cyber attack kills?

What does cyberwarfare look like?

Just like normal warfare which can range from limited skirmishes to full-on battles, the impact of cyberwarfare will vary by target and severity. In many cases the computer systems are not the final target -- they are being targeted because of their role in managing real-world infrastructure like airports or power grids. Knock out the computers

and you can shut down the airport or the power station as a result.

There are plenty of grim cyberwarfare scenarios available. Perhaps attackers start with the banks: one day your bank balance drops to zero and then suddenly leaps up, showing you've got millions in your account. Then stock prices start going crazy as hackers alter data flowing into the stock exchange. The next day the trains aren't running because the signalling stops working, and you can't drive anywhere because the traffic lights are all stuck on red, and the shops in big cities start running out of food. Pretty soon a country could be reduced to gridlock and chaos, even without the doomsday scenarios of hackers disabling power stations or opening dams.

One worst-case cyberattack scenario on the US sees attackers combining outright destructive attacks focused on critical US infrastructure with data manipulation on a massive scale.

If the race between corporate giants Amazon, Microsoft, and Walmart to create fully-automated shopping experiences is any indication, retail could look a lot different in the near future.

But are consumers ready for changes to the brick-and-mortar experience? Find out what consumers are using while shopping, whether it made the shopping experience easier (or more difficult), and what information consumers are willing to give up in exchange for special promotions or discounts.

Still, there are -- thankfully -- vanishingly few examples of real-world cyberwarfare, at least for now.

Nearly every system we use is underpinned in some way by computers, which means pretty much every aspect of our lives could be vulnerable to cyberwarfare at some point, and some experts warn it's a case of when, not if.

***Download all the Cyberwar and the Future of Cybersecurity articles as a free PDF ebook* (free TechRepublic registration required)**

Why are governments investing in cyberwarfare right now?

Governments are increasingly aware that modern societies are so reliant on computer systems to run everything from financial services to transport networks that using hackers armed with viruses or other tools to shut down those systems could be just as effective and damaging as traditional military campaign using troops armed with guns and missiles.

Unlike traditional military attacks, a cyberattack can be launched instantaneously from any distance, with little obvious evidence of any build-up, unlike a traditional military operation. Such as attack would be extremely hard to trace back with any certainty to its perpetrators, making retaliation harder.

As a result 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 are racing to improve their computer security.

However, they also see the opportunity that cyberwarfare capabilities bring, offering a new way to exert influence on rival states without having to put soldiers at risk. The fear of being vulnerable to the cyberweapons of their rivals plus a desire to harness these tools to bolster their own standing in the world is leading many countries into a cyber arms race.

- **NSA chief: This is what a worst-case cyberattack scenario looks like**
- **The impossible task of counting up the world's cyber armies**
- **Cybercrime and cyberwar: A spotter's guide to the groups that are out to get you**

What is -- and what is not -- cyberwarfare?

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

Like other forms of warfare, cyberwarfare in its purest sense is usually defined as a conflict between states, not individuals. To qualify the attacks really should be of significant scale and severity.

- **Inside the secret digital arms race: Facing the threat of a global cyberwar**
- **Governments and nation states are now officially training for cyberwarfare: An inside look**

If cyberwar is best understood as serious conflict between nations, that excludes a lot of the attacks that are regularly and incorrectly described as cyberwarfare.

Attacks by individual hackers, or even groups of hackers, would not usually be considered to be cyberwarfare, unless they are being aided and directed by a state. Still, in the murky world of cyberwarfare there are plenty of blurred lines: states providing support to hackers in order to create plausible deniability for their own actions is, however, a dangerously common trend.

Nation states' conflict is increasingly moving online.

Getty Images/iStockphoto

One 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 come 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 an individual company's website is unlikely to be considered an act of cyberwarfare, but disabling the missile defence system at an airbase would certainly come at least close.

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, even if the data center contained government records. And using hackers to spy or even to steal data would not in itself be considered an act of cyberwarfare, and would instead come under the heading cyber espionage, something which is done by nearly all governments.

For sure there are many grey areas here (cyberwarfare is basically one big grey area anyway), but calling every hack an act of cyberwar is at best unhelpful and at its worst is scaremongering that could lead to dangerous escalation.

Cyberwarfare and the use of force

Why the who, what and how of cyberwarfare matters is because how these factors combine will help determine what kind of response a country can make to a cyberattack.

There is one key formal 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 the significant threshold because under international law, countries are allowed 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, the government is within its rights to strike back using the force of their standard military arsenal: to respond to hacking with missile strikes perhaps.

So far this has never happened -- indeed it's not entirely clear if any attack has ever reached that threshold. Even if such an attack occurred it wouldn't be assumed that the victim would necessarily strike back in such a way, but international law would not stand in the way of such a response.

That doesn't mean attacks that 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 (see cyber deterrence, below).

- **In the grey area between espionage and cyberwar**
- **Russia 'front of the queue' when it comes to hacking, says security minister**

What is the Tallinn Manual?

One reason that the legal status of cyberwarfare has been blurred is that there is no international law that refers to cyberwar, because it is such a new concept. But this doesn't mean that cyberwarfare isn't covered by 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 that some states are very willing to exploit, using the opportunity to test out cyberwar techniques in the knowledge that other states are 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, the ones at the level of the use of force; the second edition released tried to build a legal framework around cyberattacks that do not reach the threshold of the use of force.

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.

The second version of the manual, know as Tallinn 2.0, looks at the legal status of the various types of hacking and other digital attacks that occur on a daily basis during peacetime and looks at when a digital attack becomes a a violation of international law in cyberspace.

- **The new art of war: How trolls, hackers and spies are rewriting the rules of conflict**
- **Did Russia's election hacking break international law? Even the experts aren't sure**

Which countries are preparing for cyberwar?

Pretty much every single nation with the money and the skills is investing in cyberwarfare and cyberdefence capabilities. According to US intelligence chiefs, more than 30 countries are developing offensive cyber attack capabilities, although most of these government hacking programmes are shrouded in secrecy. This has lead to concerns that a secret cyber arms race has already begun.

US intelligence briefings regularly list Russia, China, Iran, and North Korea as the major cyber threat actors to worry about. The US has long warned that Russia has a "highly advanced offensive cyber program" and has "conducted damaging and/or disruptive cyber attacks, including attacks on critical infrastructure networks".

The Pentagon has said that China is looking to narrow the gap with the US in terms of cyberwarfare capabilities, and has warned that China has attempted to probe US networks for data useful in any future crisis: "Targeted information could enable PLA [People's Liberation Army] cyber forces to build an operational picture of US defense networks, military disposition, logistics, and related military capabilities that could be exploited prior to or during a crisis," it warned.

- **China aims to narrow cyberwarfare gap with US**

US cyberwarfare capabilities

However, it's likely that the US still has the most significant cyberdefence and cyberattack capabilities. Speaking in 2016, President Obama said: "we're moving into a new era 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, 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".

Admiral Michael Rogers, director of the US National Security Agency and head of US Cyber Command

Image: Siim Teder/Estonian Defence Forces

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. Other US agencies like the CIA and NSA have cyber espionage 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 it is working on cyber defence and offence projects, and has vowed to strike back if attacked in this manner. In April 2018 the director of GCHQ confirmed that cyberattacks by British intelligence services supported operations against the terror group ISIS.

- British spies waged cyber campaign against ISIS, says GCHQ chief

What do cyberweapons look like?

Imaging the smartest hackers with the biggest budgets aiming to break the biggest systems they can; that's what the high end of cyber weapons can look like -- projects involving teams of developers and millions of dollars. But there are very, very few of these. In general 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 (DDoS) attack was at the core of the attacks on Estonia in 2007.

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 of 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.

Ransomware and cyberwarfare

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. Perhaps one of the most unexpected twists recently has been the use of weaponised ransomware to destroy data. The US, UK and a number of other governments blamed Russia for the NotPetya ransomware outbreak which caused havoc in mid-2017, with the White House describing the incident as

'the most destructive and costly cyberattack in history.' While the attack was most likely aimed at doing damage to computer systems in Ukraine it rapidly spread further and caused billions of dollars of damage, reflecting how easily cyber weapons can get beyond the control of their makers.

- **Blaming Russia for NotPetya was coordinated diplomatic action**
- **'Russian military behind NotPetya attacks': UK officially names and shames Kremlin**
- **NotPetya cyber attack on TNT Express cost FedEx $300m**
- **NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs**

Cyberwarfare and zero-day attack stockpiles

Zero-day vulnerabilities are bugs or flaws in code that 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 cyber weapons, particularly those using zero-day exploits is that -- unlike a conventional bomb or missile -- a cyber weapon 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 that had been stockpiled by the NSA, presumably to use in cyber espionage. But the tool was somehow acquired by the Shadow Brokers hacking group (quite how is extremely unclear) which then leaked it online. Once this happened other ransomware writers incorporated it into their software, making it vastly more powerful.

This risk of unexpected consequences mean that cyber weapons 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 and also cause much greater chaos than planned, which is what may have happened in the case of the Ukrainian NotPetya ransomware attack.

What is Stuxnet?

Image: Getty Images/iStockphoto

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 cyber weapons may mean cyber conflicts 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.

- **The spy on the corner of your desk: Why the smart office is your next security nightmare**

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 cyber defence 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. Not all IoT devices are in homes; hospitals and factories and smart cities are now filled with sensors and other devices which means that the real-world impact of an IoT

outage could be widely felt.

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.

At a higher level, nations and groups of states are developing their own cyber defence strategies. The European Union recently announced plans to work on a cyber defence plan which it will invoke if it faces a major, cross-border cyberattack, and plans to work with NATO on cyber defence exercises. However, not all nations consider such planning to be a particularly high priority.

More broadly, to prevent cyberwar incidents, countries need to talk more: to understand where the boundaries lie and which kinds of behaviour are acceptable. Until that is done there is always the risk of misunderstanding and escalation.

What is cyber deterrence?

Just as nations attempt to deter rivals from attacking in conventional weapons, so countries are developing the concept of cyber deterrence to help to prevent digital attacks from occurring in the first place -- by making the cost of the attack too high for any potential assailant.

One way of doing that is securing and hardening their own computer systems so that is becomes very hard -- and very expensive -- for any attacker to find weaknesses. Thanks to the swiss-cheese nature of so many computer systems the attackers will still have the advantage here.

The other option is to impose costs on the attackers through sanctions, criminal investigations or even the threat of striking back. Most recently the US in particular has been attempting to create deterrence through a policy of naming-and-shaming, in particular using indictments to name particular individuals it believes are responsible for carrying out state-backed cyber attacks.However, as hackers (from all nations) continue to poke and pry at the computer systems of their rivals, it would seem that cyber deterrence is at best a work in progress.

- Can Russian hackers be stopped? Here's why it might take 20 years
- Russian election meddling continues, says US: So why can't it be stopped?

What is cyber espionage?

Closely related but separate to cyberwarfare is cyber espionage, 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 cyber espionage 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 cyber espionage 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," then-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 as a result.

What are cyber wargames?

A member of the Locked Shields Green Team during the cyber defence exercise.

Image: NATO

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

Some of biggest international cyber defence 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.

It's not just the technical aspects of cyberwarfare that are tested out; in September 2017 European Union defence ministers also took place in a table-top exercise called EU Cybrid, designed to test their strategy and decision making in the face of a major cyberattack on the European Union military organisations. The game aimed to help develop guidelines to be used in such a real-life crisis, and was the first exercise to involve politicians at such a senior level.

When will cyberwar take place?

Some argue cyberwar will never take place; others argue cyberwar is taking place right now. The truth is of course somewhere in the middle.

Beyond the famous example of Stuxnet pure cyberwar operations will remain extremely rare, but already the concept has become absorbed into the broader set of military options that exist, just like other new technologies, such as submarines and aircraft, in the past.

It's possible that cyber weapons may also become a more common feature of low intensity skirmishes between nations because they are capable of causing confusion and chaos but not (too) much damage. But it's unlikely that a war would ever be fought purely with digital weapons because they are too expensive and hard to control and of limited impact.

That doesn't mean cyberwarfare is irrelevant -- rather that some kind of cyberwarfare capability will be part of pretty much every military engagement from now on.

Read more on cyberwarfare

- Governments and nation states are now officially training for cyberwarfare: An inside look
- The new art of war: How trolls, hackers and spies are rewriting the rules of conflict
- Inside the secret digital arms race: Facing the threat of a global cyberwar
- The undercover war on your internet secrets: How online surveillance cracked our trust in the web
- The impossible task of counting up the world's cyber armies
- Cybercrime and cyberwar: A spotter's guide to the groups that are out to get you
- In the grey area between espionage and cyberwar
- NSA chief: This is what a worst-case cyberattack scenario looks like
- Why the CIA's iOS, Android and Windows hack stockpile puts zero-day hoards in the spotlight
- Did Russia's election hacking break international law? Even the experts aren't sure
- From malware to cyber-spies, the 15 biggest threats online, ranked
- Russian hackers target critical infrastructure and democracy, warns UK
- The hackers that never went away: Brace for more state-backed attacks, leaks and copycats this year
- US intelligence: 30 countries building cyber attack capabilities
- Cyberwar: The smart person's guide (TechRepublic)