Cyberwarfare

Cyberwarfare is the use of cyber attacks against an enemy state, causing comparable harm to actual warfare and/or disrupting vital computer systems.[1] Some intended outcomes could be espionage, sabotage, propaganda, manipulation or economic warfare.

There is significant debate among experts regarding the definition of cyberwarfare, and even if such a thing exists.[2] One view is that the term is a misnomer, since no cyber attacks to date could be described as war.[3] An alternative view is that it is a suitable label for cyber attacks which cause physical damage to people and objects in the real world.[4]

Many countries including the United States, United Kingdom, Russia, China, Israel, Iran, and North Korea[5][6][7][8] have active cyber capabilities for offensive and defensive operations. As states explore the use of cyber operations and combine capabilities the likelihood of physical confrontation and violence playing out as a result of, or part of, a cyber operation is increased. However, meeting the scale and protracted nature of war is unlikely, thus ambiguity remains.[9]

The first instance of kinetic military action used in response to a cyber-attack resulting in the loss of human life was observed on 5 May 2019, when the Israel Defense Forces targeted and destroyed a building associated with an ongoing cyber-attack.[10][11]

Definition

There is ongoing debate over how cyberwarfare should be defined and no absolute definition is widely agreed upon.[9][12] While the majority of scholars, militaries and governments use

definitions which refer to state and state-sponsored actors,[9][13][14] other definitions may include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations depending on the context of the work.[15][16]

Examples of definitions proposed by experts in the field are as follows.

> 'Cyberwarfare' is used in a broad context to denote interstate use of technological force within computer networks in which information is stored, shared or communicated online.[9]

Parks and Duggan focused on analyzing cyberwarfare in terms of computer networks and pointed out that "Cyberwarfare is a combination of computer network attack and defense and special technical operations."[17] According to this perspective, the notion of cyberwarfare brings a new paradigm into the military doctrine. Paulo Shakarian and colleagues, put forward the following definition in 2013 drawing from various works including Clausewitz's definition of war: "War is the continuation of politics by other means":[13]

> "Cyberwarfare is an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived)."

Taddeo offered the following definition in 2012:

> "The warfare grounded on certain uses of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemys resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances".[18]

Robinson et al. proposed in 2015, that the intent of the attacker dictates whether an attack is warfare or not, defining cyber warfare as "the use of cyber attacks with a warfare-like intent."[12]

In 2010, the former US National Coordinator for Security, Infrastructure Protection and Counter-terrorism, Richard A. Clarke, defined cyberwarfare as "actions by a nation-state to penetrate

another nation's computers or networks for the purposes of causing damage or disruption."[14] Own cyber-physical infrastructure may be weaponized and used by the adversary in case of a cyber conflict, thus turning such infrastructure into tactical weapons.[19]

Controversy of term

There is debate on whether the term "cyberwarfare" is accurate. In 2012, Eugene Kaspersky, founder of Kaspersky Lab, concludes that "cyberterrorism" is a more accurate term than "cyberwar". He states that "with today's attacks, you are clueless about who did it or when they will strike again. It's not cyber-war, but cyberterrorism."[20] Howard Schmidt, former Cyber Security Coordinator of the Obama Administration, said that "there is no cyberwar... I think that is a terrible metaphor and I think that is a terrible concept. There are no winners in that environment."[21]

Some experts take issue with the possible consequences linked to the warfare analogy. In 2011, Ron Deibert, of Canada's Citizen Lab, has warned of a "militarization of cyberspace", as militaristic responses may not be appropriate.[22] Although, to date, even serious cyber attacks which have disrupted large parts of a nations electrical grids (230,000 customers, Ukraine, 2015) or affected access to medical care, thus endangering life (NHS, WannaCry, 2017) have not led to military action.

In 2017, Oxford academic Lucas Kello proposed a new term – "Unpeace" – to denote highly damaging cyber actions whose non-violent effects do not rise to the level of traditional war. Such actions are neither warlike nor peace like. Although they are non-violent, and thus not acts of war, their damaging effects on the economy and society may be greater than even some armed attacks.[23][24] This term is closely related to the concept of the "grey zone" which has come to prominence in 2017, describing actions which fall below the traditional threshold of war.[25]

Cyberwarfare vs. cyber war

The term "cyberwarfare" is distinct from the term "cyber war". "Cyberwarfare" does not imply scale, protraction or violence which are typically associated with the term "war".[9] Cyber warfare includes techniques, tactics and procedures which may be involved in a cyber war. The term war inherently refers to a large scale action, typically over a protracted period of time and may include objectives seeking to utilize violence or the aim to kill.[9] A cyber war could accurately

describe a protracted period of back-and-forth cyber attacks (including in combination with traditional military action) between warring states. To date, no such action is known to have occurred. Instead, tit-for-tat military-cyber actions are more commonplace. For example, in June 2019, the United States launched a cyber attack against Iranian weapons systems in retaliation to the shooting down of a US drone being in the Strait of Hormuz.[26][27]

Cyberwarfare and cyber sanctions

The use of digital attacks, as described by the concept of cyberwarfare, in this page can be a retaliatory response to the cyber attacks. In addition, countries can use cyber sanctions as a reaction to being the targets of the cyber attacks. Sometimes, it is not easy to detect the attacker; however, it might be the case that suspicions can focus on a certain country or group of countries. In these cases, unilateral and multilateral economic sanctions can be used instead of cyberwarfare. For example, economic sanctions related to cyber attacks have been frequently used by the United States government. There are two Executive Orders, EO 13694[28] in 2015 and EO 13757[29][30] in 2016, issued during the Obama administration specifically focused on the implementation of the cyber sanctions. Later on, these Executive Orders have been frequently used by the following US presidents. Furthermore, the Congress is an important actor when it comes to the cyber sanctions. For example, Iran Cyber Sanctions Act of 2016 is a bill that imposes sanctions on specific individuals responsible for the cyber attacks.[31]

Types of threat

Types of warfare

Cyber warfare can present a multitude of threats towards a nation. At the most basic level, cyber attacks can be used to support traditional warfare. For example, tampering with the operation of air defenses via cyber means in order to facilitate an air attack.[32] Aside from these "hard" threats, cyber warfare can also contribute towards "soft" threats such as espionage and propaganda. Eugene Kaspersky, founder of Kaspersky Lab, equates large-scale cyber weapons, such as Flame and NetTraveler which his company discovered, to biological weapons, claiming that in an interconnected world, they have the potential to be equally destructive.[20][33]

Espionage

PRISM: a clandestine surveillance program under which the NSA collects user data from companies like Facebook and Google.

Traditional espionage is not an act of war, nor is cyber-espionage, and both are generally assumed to be ongoing between major powers.[34] Despite this assumption, some incidents can cause serious tensions between nations, and are often described as "attacks". For example:[35]

- Massive spying by the US on many countries, revealed by Edward Snowden.
- After the NSA's spying on Germany's Chancellor Angela Merkel was revealed, the Chancellor compared the NSA with the Stasi.[36]
- The NSA recording nearly every cell phone conversation in the Bahamas, without the Bahamian government's permission, and similar programs in Kenya, the Philippines, Mexico and Afghanistan.[37][38]
- The "Titan Rain" probes of American defense contractors computer systems since 2003.[39]
- The Office of Personnel Management data breach, in the US, widely attributed to China.[40][41]
- The security firm Area 1 published details of a breach that compromised one of the European Union's diplomatic communication channels for three years.[42]

Out of all cyber attacks, 25% of them are espionage based.

Sabotage

Computers and satellites that coordinate other activities are vulnerable components of a system and could lead to the disruption of equipment. Compromise of military systems, such as C4ISTAR components that are responsible for orders and communications could lead to their

interception or malicious replacement. Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption. According to Clarke, the civilian realm is also at risk, noting that the security breaches have already gone beyond stolen credit card numbers, and that potential targets can also include the electric power grid, trains, or the stock market.[43]

In mid-July 2010, security experts discovered a malicious software program called Stuxnet that had infiltrated factory computers and had spread to plants around the world. It is considered "the first attack on critical industrial infrastructure that sits at the foundation of modern economies," notes *The New York Times*.[44]

Stuxnet, while extremely effective in delaying Iran's nuclear program for the development of nuclear weaponry, came at a high cost. For the first time, it became clear that not only could cyber weapons be defensive but they could be offensive. The large decentralization and scale of cyberspace makes it extremely difficult to direct from a policy perspective. Non-state actors can play as large a part in the cyberwar space as state actors, which leads to dangerous, sometimes disastrous, consequences. Small groups of highly skilled malware developers are able to as effectively impact global politics and cyber warfare as large governmental agencies. A major aspect of this ability lies in the willingness of these groups to share their exploits and developments on the web as a form of arms proliferation. This allows lesser hackers to become more proficient in creating the large scale attacks that once only a small handful were skillful enough to manage. In addition, thriving black markets for these kinds of cyber weapons are buying and selling these cyber capabilities to the highest bidder without regard for consequences.[45][46]

Denial-of-service attack

In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. DoS attacks often leverage internet-connected devices with vulnerable security measures to carry out these large-scale attacks.[47] DoS attacks may not be limited to computer-based methods, as strategic physical attacks against infrastructure can be just as devastating. For example, cutting undersea communication cables may severely cripple some regions and countries with regards to their information warfare ability.

A Grid Transformer Station

Electrical power grid

The federal government of the United States admits that the electric power grid is susceptible to cyberwarfare.[48][49] The United States Department of Homeland Security works with industries to identify vulnerabilities and to help industries enhance the security of control system networks. The federal government is also working to ensure that security is built in as the next generation of "smart grid" networks are developed.[50] In April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national security officials.[51] The North American Electric Reliability Corporation (NERC) has issued a public notice that warns that the electrical grid is not adequately protected from cyber attack.[52] China denies intruding into the U.S. electrical grid.[53] One countermeasure would be to disconnect the power grid from the Internet and run the net with droop speed control only.[54] Massive power outages caused by a cyber attack could disrupt the economy, distract from a simultaneous military attack, or create a national trauma.

Iranian hackers, possibly Iranian Cyber Army pushed a massive power outage for 12 hours in 44 of 81 provinces of Turkey, impacting 40 million people. Istanbul and Ankara were among the places suffering blackout.[55]

Howard Schmidt, former Cyber-Security Coordinator of the US, commented on those possibilities:[21]

> It's possible that hackers have gotten into administrative computer systems of utility companies, but says those aren't linked to the equipment

> controlling the grid, at least not in developed countries. [Schmidt] has never heard that the grid itself has been hacked.

In June 2019, Russia said that its electrical grid has been under cyber-attack by the United States. The *New York Times* reported that American hackers from the United States Cyber Command planted malware potentially capable of disrupting the Russian electrical grid.[56]

Propaganda

Cyber propaganda is an effort to control information in whatever form it takes, and influence public opinion.[57] It is a form of psychological warfare, except it uses social media, fake news websites and other digital means.[58] In 2018, Sir Nicholas Carter, Chief of the General Staff of the British Army stated that this kind of attack from actors such as Russia "is a form of system warfare that seeks to de-legitimize the political and social system on which our military strength is based".[59]

Jowell and O'Donnell (2006) state that "propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist" (p. 7). The internet is the most important means of communication today. People can convey their messages quickly across to a huge audience, and this can open a window for evil. Terrorist organizations can exploit this and may use this medium to brainwash people. It has been suggested that restricted media coverage of terrorist attacks would in turn decrease the number of terrorist attacks that occur afterwards.[60]

Economic disruption

In 2017, the WannaCry and Petya (NotPetya) cyber attacks, masquerading as ransomware, caused large-scale disruptions in Ukraine as well as to the U.K.'s National Health Service, pharmaceutical giant Merck, Maersk shipping company and other organizations around the world.[61][62][63] These attacks are also categorized as cybercrimes, specifically financial crime because they negatively affect a company or group.

Surprise cyber attack

The idea of a "cyber Pearl Harbor" has been debated by scholars, drawing an analogy to the historical act of war.[64][65][66][67][68] Others have used "cyber 9/11" to draw attention to the

nontraditional, asymmetric, or irregular aspect of cyber action against a state.[69][70]

Motivations

There are a number of reasons nations undertake offensive cyber operations. Sandro Gaycken, a cyber security expert and adviser to NATO, advocates that states take cyber warfare seriously as they are viewed as an attractive activity by many nations, in times of war and peace. Offensive cyber operations offer a large variety of cheap and risk-free options to weaken other countries and strengthen their own positions. Considered from a long-term, geostrategic perspective, cyber offensive operations can cripple whole economies, change political views, agitate conflicts within or among states, reduce their military efficiency and equalize the capacities of high-tech nations to that of low-tech nations, and use access to their critical infrastructures to blackmail them.[71]

Military

With the emergence of cyber as a substantial threat to national and global security, cyber war, warfare and/or attacks also became a domain of interest and purpose for the Military.

In the U.S., General Keith B. Alexander, first head of USCYBERCOM, told the Senate Armed Services Committee that computer network warfare is evolving so rapidly that there is a "mismatch between our technical capabilities to conduct operations and the governing laws and policies. Cyber Command is the newest global combatant and its sole mission is cyberspace, outside the traditional battlefields of land, sea, air and space." It will attempt to find and, when necessary, neutralize cyberattacks and to defend military computer networks.[72]

Alexander sketched out the broad battlefield envisioned for the computer warfare command, listing the kind of targets that his new headquarters could be ordered to attack, including "traditional battlefield prizes – command-and-control systems at military headquarters, air defense networks and weapons systems that require computers to operate."[72]

One cyber warfare scenario, Cyber-ShockWave, which was wargamed on the cabinet level by former administration officials, raised issues ranging from the National Guard to the power grid to the limits of statutory authority.[73][74][75][76]

The distributed nature of internet based attacks means that it is difficult to determine motivation and attacking party, meaning that it is unclear when a specific act should be considered an act

of war.[77]

Examples of cyberwarfare driven by political motivations can be found worldwide. In 2008, Russia began a cyber attack on the Georgian government website, which was carried out along with Georgian military operations in South Ossetia. In 2008, Chinese "nationalist hackers" attacked CNN as it reported on Chinese repression on Tibet.[78] Hackers from Armenia and Azerbaijan have actively participated in cyberwarfare as part of the Nagorno-Karabakh conflict, with Azerbaijani hackers targeting Armenian websites and posting Ilham Aliyev's statements.[79][80]

Jobs in cyberwarfare have become increasingly popular in the military. All four branches of the United States military actively recruit for cyber warfare positions.[81]

As the military have become more and more entangled into the national and global threat proposed by the utilization of the cyber domain, a new research field within the Military Science field have slowly emerged. In essence, its focus is centered towards describing, understanding and explaining what **Military Cyber Operations** is, can do and be tackled. In the *Handbook of Military Sciences* Aaron Brantly and Max Smeets define Military Cyber Operations to be "those cyber operations which a military entity of a nation-state plans and conducts to achieve strategic, operational, or tactical gain."[82] More so, they argue these types of military operations are commonly divided into three types of operations.

- *Defensive Cyber Operations*: Encompassing "those actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within a governments information systems and computer networks"."[82]
- *Cyber Espionage Operations*: Encompassing "those actions taken through the use of computer networks to gather data from target or adversary information systems or network"."[82][83]
- *Offensive Cyber Operations*: Encompassing "those actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves, or in basic, operations designed to achieve tangible effects"."[82][84][85]

Civil

Potential targets in internet sabotage include all aspects of the Internet from the backbones of the web, to the internet service providers, to the varying types of data communication mediums and network equipment. This would include: web servers, enterprise information systems, client server systems, communication links, network equipment, and the desktops and laptops in

businesses and homes. Electrical grids, financial networks, and telecommunication systems are also deemed vulnerable, especially due to current trends in computerization and automation.[86]

Hacktivism

Politically motivated hacktivism involves the subversive use of computers and computer networks to promote an agenda, and can potentially extend to attacks, theft and virtual sabotage that could be seen as cyberwarfare – or mistaken for it.[87] Hacktivists use their knowledge and software tools to gain unauthorized access to computer systems they seek to manipulate or damage not for material gain or to cause widespread destruction, but to draw attention to their cause through well-publicized disruptions of select targets. Anonymous and other hacktivist groups are often portrayed in the media as cyber-terrorists, wreaking havoc by hacking websites, posting sensitive information about their victims, and threatening further attacks if their demands are not met. However, hacktivism is more than that. Actors are politically motivated to change the world, through the use of fundamentalism. Groups like Anonymous, however, have divided opinion with their methods.[88]

Income generation

Cyber attacks, including ransomware, can be used to generate income. States can use these techniques to generate significant sources of income, which can evade sanctions and perhaps while simultaneously harming adversaries (depending on targets). This tactic was observed in August 2019 when it was revealed North Korea had generated $2 billion to fund its weapons program, avoiding the blanket of sanctions levied by the United States, United Nations and the European Union.[89][90]

Private sector

Computer hacking represents a modern threat in ongoing global conflicts and industrial espionage and as such is presumed to widely occur.[86] It is typical that this type of crime is underreported to the extent they are known. According to McAfee's George Kurtz, corporations around the world face millions of cyberattacks a day. "Most of these attacks don't gain any media attention or lead to strong political statements by victims."[91] This type of crime is usually financially motivated.

Non-profit research

But not all those who engage in cyberwarfare do so for financial or ideological reasons. There are institutes and companies like the University of Cincinnati[92] or the Kaspersky Security Lab which engage in cyberwarfare so as to better understand the field through actions like the researching and publishing of new security threats.

Preparedness

A number of countries conduct exercise to increase preparedness and explore the strategy, tactics and operations involved in conducting and defending against cyber attacks against hostile states, this is typically done in the form of war games.

The Cooperative Cyber Defence Centre of Excellence (CCDCE), part of the North Atlantic Treaty Organization (NATO), have conducted a yearly war game called Locked Shields since 2010 designed to test readiness and improve skills, strategy tactics and operational decision making of participating national organizations.[93][94] Locked Shields 2019 saw 1200 participants from 30 countries compete in a red team vs. blue team exercise. The war game involved a fictional country, Berylia, which was "experiencing a deteriorating security situation, where a number of hostile events coincide with coordinated cyber attacks against a major civilian internet service provider and maritime surveillance system. The attacks caused severe disruptions in the power generation and distribution, 4G communication systems, maritime surveillance, water purification plant and other critical infrastructure components". CCDCE describe the aim of the exercise was to "maintain the operation of various systems under intense pressure, the strategic part addresses the capability to understand the impact of decisions made at the strategic and policy level."[93][95] Ultimately, France was the winner of Locked Shields 2019.[96]

The European Union conducts cyber war game scenarios with member states and foreign partner states to improve readiness, skills and observe how strategic and tactical decisions may affect the scenario.[97]

As well as war games which serve a broader purpose to explore options and improve skills, cyber war games are targeted at preparing for specific threats. In 2018 the Sunday Times reported the UK government was conducting cyber war games which could "blackout Moscow".[98][99] These types of war games move beyond defensive preparedness, as previously described above and onto preparing offensive capabilities which can be used as deterrence, or for "war".

Cyber activities by nation

Approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.[100]

Asia

China

Foreign Policy magazine puts the size of China's "hacker army" at anywhere from 50,000 to 100,000 individuals.[101]

Diplomatic cables highlight US concerns that China is using access to Microsoft source code and 'harvesting the talents of its private sector' to boost its offensive and defensive capabilities.[102]

The 2018 cyberattack on the Marriott hotel chain[103][104] that collected personal details of roughly 500 million guests is now known to be a part of a Chinese intelligence-gathering effort that also hacked health insurers and the security clearance files of millions more Americans, The hackers, are suspected of working on behalf of the Ministry of State Security, the country's Communist-controlled civilian spy agency.[105][106][107] "The information is exactly what the Chinese use to root out spies, recruit intelligence agents and build a rich repository of Americans' personal data for future targeting."

A 2008 article in the *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies* by Jason Fritz alleges that the Chinese government from 1995 to 2008 was involved in a number of high-profile cases of espionage, primarily through the use of a "decentralized network of students, business people, scientists, diplomats, and engineers from within the Chinese Diaspora".[108] A defector in Belgium, purportedly an agent, claimed that there were hundreds of spies in industries throughout Europe, and on his defection to Australia Chinese diplomat Chen Yonglin said there were over 1,000 such in that country. In 2007, a Russian executive was sentenced to 11 years for passing information about the rocket and space technology organization to China. Targets in the United States have included "aerospace engineering programs, space shuttle design, C4ISR data, high-performance computers, Nuclear weapon design, cruise missile data, semiconductors, integrated circuit design, and details of US arms sales to Taiwan".[108]

While China continues to be held responsible for a string of cyber-attacks on a number of public and private institutions in the United States, India, Russia, Canada, and France, the Chinese government denies any involvement in cyber-spying campaigns. The administration maintains the position that China is not the threat but rather the victim of an increasing number of cyber-attacks. Most reports about China's cyber warfare capabilities have yet to be confirmed by the Chinese government.[109]

According to Fritz, China has expanded its cyber capabilities and military technology by acquiring foreign military technology.[110] Fritz states that the Chinese government uses "new space-based surveillance and intelligence gathering systems, Anti-satellite weapon, anti-radar, infrared decoys, and false target generators" to assist in this quest, and that they support their "Informatisation" of their military through "increased education of soldiers in cyber warfare; improving the information network for military training, and has built more virtual laboratories, digital libraries and digital campuses."[110] Through this informatisation, they hope to prepare their forces to engage in a different kind of warfare, against technically capable adversaries.[111] Many recent news reports link China's technological capabilities to the beginning of a new "cyber cold war."[112]

Operation Shady RAT is an ongoing series of cyber attacks starting mid-2006, reported by Internet security company McAfee in August 2011. China is widely believed to be the state actor behind these attacks which hit at least 72 organizations including governments and defense contractors.[113]

On 14 September 2020, a database showing personal details of about 2.4 million people around the world was leaked and published. A Chinese company, Zhenhua Data Information Technology Co., Ltd. compiled the database.[114] According to the information from "National Enterprise Credit Information Publicity System", which is run by State Administration for Market Regulation in China, the shareholders of Zhenhua Data Information Technology Co., Ltd. are two natural persons and one general partnership enterprise whose partners are natural persons.[115] Wang Xuefeng, who is the chief executive and the shareholder of Zhenhua Data, has publicly boasted that he supports "hybrid warfare" through manipulation of public opinion and "psychological warfare".[116]

India

The Department of Information Technology created the Indian Computer Emergency Response Team (CERT-In) in 2004 to thwart cyber attacks in India.[117] That year, there were 23 reported cyber security breaches. In 2011, there were 13,301. That year, the government created a new

subdivision, the National Critical Information Infrastructure Protection Centre (NCIIPC) to thwart attacks against energy, transport, banking, telecom, defense, space and other sensitive areas.

The Executive Director of the Nuclear Power Corporation of India (NPCIL) stated in February 2013 that his company alone was forced to block up to ten targeted attacks a day. CERT-In was left to protect less critical sectors.

A high-profile cyber attack on 12 July 2012 breached the email accounts of about 12,000 people, including those of officials from the Ministry of External Affairs, Ministry of Home Affairs, Defense Research and Development Organizations (DRDO), and the Indo-Tibetan Border Police (ITBP).[117] A government-private sector plan being overseen by National Security Advisor (NSA) Shivshankar Menon began in October 2012, and intends to boost up India's cyber security capabilities in the light of a group of experts findings that India faces a 470,000 shortfall of such experts despite the country's reputation of being an IT and software powerhouse.[118]

In February 2013, Information Technology Secretary J. Satyanarayana stated that the NCIIPC was finalizing policies related to national cyber security that would focus on domestic security solutions, reducing exposure through foreign technology.[117] Other steps include the isolation of various security agencies to ensure that a synchronised attack could not succeed on all fronts and the planned appointment of a National Cyber Security Coordinator. As of that month, there had been no significant economic or physical damage to India related to cyber attacks.

On 26 November 2010, a group calling itself the Indian Cyber Army hacked the websites belonging to the Pakistan Army and the others belong to different ministries, including the Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The attack was done as a revenge for the Mumbai terrorist attacks.[119]

On 4 December 2010, a group calling itself the Pakistan Cyber Army hacked the website of India's top investigating agency, the Central Bureau of Investigation (CBI). The National Informatics Center (NIC) has begun an inquiry.[120]

In July 2016, Cymmetria researchers discovered and revealed the cyber attack dubbed 'Patchwork', which compromised an estimated 2500 corporate and government agencies using code stolen from GitHub and the dark web. Examples of weapons used are an exploit for the Sandworm vulnerability (CVE-2014-4114 (https://www.cve.org/CVERecord?id=CVE-2014-4114)), a compiled AutoIt script, and UAC bypass code dubbed UACME. Targets are believed to be mainly military and political assignments around Southeast Asia and the South China Sea and

the attackers are believed to be of Indian origin and gathering intelligence from influential parties.[121][122]

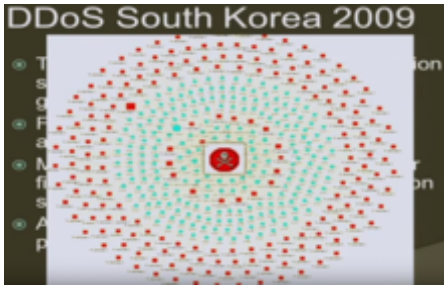
The Defence Cyber Agency, which is the Indian Military agency responsible for Cyberwarfare, is expected to become operational by November 2019.[123]

Philippines

The Chinese are being blamed after a cybersecurity company, F-Secure Labs, found a malware, NanHaiShu, which targeted the Philippines Department of Justice. It sent information in an infected machine to a server with a Chinese IP address. The malware which is considered particularly sophisticated in nature was introduced by phishing emails that were designed to look like they were coming from an authentic sources. The information sent is believed to be relating to the South China Sea legal case.[124]

South Korea

In July 2009, there were a series of coordinated denial of service attacks against major government, news media, and financial websites in South Korea and the United States.[125] While many thought the attack was directed by North Korea, one researcher traced the attacks to the United Kingdom.[126] Security researcher Chris Kubecka presented evidence multiple European Union and United Kingdom companies unwittingly helped attack South Korea due to a W32.Dozer infections, malware used in part of the attack. Some of the companies used in the attack were partially owned by several governments, further complicating attribution.[127]



Visualization of 2009 cyber warfare attacks against South Korea

In July 2011, the South Korean company SK Communications was hacked, resulting in the theft of the personal details (including names, phone numbers, home and email addresses and resident registration numbers) of up to 35 million people. A trojaned software update was used to gain access to the SK Communications network. Links exist between this hack and other malicious activity and it is believed to be part of a broader, concerted hacking effort.[128]

With ongoing tensions on the Korean Peninsula, South Korea's defense ministry stated that South Korea was going to improve cyber-defense strategies in hopes of preparing itself from possible cyber attacks. In March 2013, South Korea's major banks – Shinhan Bank, Woori Bank and NongHyup Bank – as well as many broadcasting stations – KBS, YTN and MBC – were hacked and more than 30,000 computers were affected; it is one of the biggest attacks South Korea has faced in years.[129] Although it remains uncertain as to who was involved in this incident, there has been immediate assertions that North Korea is connected, as it threatened to attack South Korea's government institutions, major national banks and traditional newspapers numerous times – in reaction to the sanctions it received from nuclear testing and to the continuation of Foal Eagle, South Korea's annual joint military exercise with the United States. North Korea's cyber warfare capabilities raise the alarm for South Korea, as North Korea is increasing its manpower through military academies specializing in hacking. Current figures state that South Korea only has 400 units of specialized personnel, while North Korea has more than 3,000 highly trained hackers; this portrays a huge gap in cyber warfare capabilities and sends a message to South Korea that it has to step up and strengthen its Cyber Warfare Command forces. Therefore, in order to be prepared from future attacks, South Korea and the United States will discuss further about deterrence plans at the Security Consultative Meeting (SCM). At SCM, they plan on developing strategies that focuses on accelerating the deployment of ballistic missiles as well as fostering its defense shield program, known as the Korean Air and Missile Defense.[130]

Sri Lanka

North Korea

Africa

Egypt

In an extension of a bilateral dispute between Ethiopia and Egypt over the Grand Ethiopian Renaissance Dam, Ethiopian government websites have been hacked by the Egypt-based hackers in June 2020.[131][132]

Europe

Cyprus

The New York Times published an exposé revealing an extensive three-year phishing campaign aimed against diplomats based in Cyprus. After accessing the state system the hackers had access to the European Union's entire exchange database.[133] By login into Coreu, hackers accessed communications linking all EU states, on both sensitive and not so sensitive matters. The event exposed poor protection of routine exchanges among European Union officials and a coordinated effort from a foreign entity to spy on another country. "After over a decade of experience countering Chinese cyberoperations and extensive technical analysis, there is no doubt this campaign is connected to the Chinese government", said Blake Darche, one of the Area 1 Security experts - the company revealing the stolen documents. The Chinese Embassy in the US did not return calls for comment.[134] In 2019, another coordinated effort took place that allowed hackers to gain access to government (gov.cy) emails. Cisco's Talos Security Department revealed that "Sea Turtle" hackers carried out a broad piracy campaign in the DNS countries, hitting 40 different organizations, including Cyprus.[135]

Estonia

In April 2007, Estonia came under cyber attack in the wake of relocation of the Bronze Soldier of Tallinn.[136] The largest part of the attacks were coming from Russia and from official servers of the authorities of Russia.[137] In the attack, ministries, banks, and media were targeted.[138][139] This attack on Estonia, a seemingly small Baltic state, was so effective because of how most of Estonian government services are run online. Estonia has implemented an e-government, where bank services, political elections and taxes, and pretty much anything modern society is now all done online.[140]

France

In 2013, the French Minister of Defense, Mr Jean-Yves Le Drian, ordered the creation of a cyber army, representing its fourth national army corp[141] (along with ground, naval and air forces) under the French Ministry of Defense, to protect French and European interests on its soil and abroad.[142] A contract was made with French firm EADS (Airbus) to identify and secure its main elements susceptible to cyber threats.[143] In 2016 France had planned 2600 "cyber-soldiers" and a 440 million euros investment for cybersecurity products for this new army corp.[144] An additional 4400 reservists constitute the heart of this army from 2019.[145]

Germany

In 2013, Germany revealed the existence of their 60-person Computer Network Operation unit.[146] The German intelligence agency, BND, announced it was seeking to hire 130 "hackers" for a new "cyber defence station" unit. In March 2013, BND president Gerhard Schindler announced that his agency had observed up to five attacks a day on government authorities, thought mainly to originate in China. He confirmed the attackers had so far only accessed data and expressed concern that the stolen information could be used as the basis of future sabotage attacks against arms manufacturers, telecommunications companies and government and military agencies.[147] Shortly after Edward Snowden leaked details of the U.S. National Security Agency's cyber surveillance system, German Interior Minister Hans-Peter Friedrich announced that the BND would be given an additional budget of 100 million Euros to increase their cyber surveillance capability from 5% of total internet traffic in Germany to 20% of total traffic, the maximum amount allowed by German law.[148]

Greece

Greek hackers from Anonymous Greece targeted Azerbaijani governmental websites during the 2020 Nagorno-Karabakh conflict between Armenia and Azerbaijan.[149]

Netherlands

In the Netherlands, Cyber Defense is nationally coordinated by the National Cyber Security Centrum (NCSC).[150] The Dutch Ministry of Defense laid out a cyber strategy in 2011.[151] The first focus is to improve the cyber defense handled by the Joint IT branch (JIVC). To improve intel operations, the intel community in the Netherlands (including the military intel organization, MIVD) has set up the Joint Sigint Cyber Unit (JSCU). The Ministry of Defense oversees an offensive cyber force, called Defensive Cyber Command (DCC).[152]

Norway

Russia

Russian, South Ossetian, Georgian and Azerbaijani sites were attacked by hackers during the 2008 South Ossetia War.[153]

American-led cyberattacks against Soviet Union and Russia

When Russia was still a part of the Soviet Union in 1982, a portion of a Trans-Siberia pipeline within its territory exploded,[154] allegedly due to a Trojan Horse computer malware implanted in the pirated Canadian software by the Central Intelligence Agency. The malware caused the SCADA system running the pipeline to malfunction. The "Farewell Dossier" provided information on this attack, and wrote that compromised computer chips would become a part of Soviet military equipment, flawed turbines would be placed in the gas pipeline, and defective plans would disrupt the output of chemical plants and a tractor factory. This caused the "most monumental nonnuclear explosion and fire ever seen from space." However, the Soviet Union did not blame the United States for the attack.[155]

In June 2019, the *New York Times* reported that American hackers from the United States Cyber Command planted malware potentially capable of disrupting the Russian electrical grid.[56]

Russian-led cyberattacks

It has been claimed that Russian security services organized a number of denial of service attacks as a part of their cyber-warfare against other countries,[156] most notably the 2007 cyberattacks on Estonia and the 2008 cyberattacks on Russia, South Ossetia, Georgia, and Azerbaijan.[157] One identified young Russian hacker said that he was paid by Russian state security services to lead hacking attacks on NATO computers. He was studying computer sciences at the *Department of the Defense of Information*. His tuition was paid for by the FSB.[158]

Sweden

In January 2017, Sweden's armed forces were subjected to a cyber-attack that caused them to shutdown a so-called Caxcis IT system used in military exercises.[159]

Ukraine

According to CrowdStrike from 2014 to 2016, the Russian APT Fancy Bear used Android malware to target the Ukrainian Army's Rocket Forces and Artillery. They distributed an infected version of an Android app whose original purpose was to control targeting data for the D-30 Howitzer artillery. The app, used by Ukrainian officers, was loaded with the X-Agent spyware and posted online on military forums. The attack was claimed by Crowd-Strike to be successful, with more than 80% of Ukrainian D-30 Howitzers destroyed, the highest percentage loss of any artillery pieces in the army (a percentage that had never been previously reported and would mean the loss of nearly the entire arsenal of the biggest artillery piece of the Ukrainian Armed Forces[160]).[161] According to the Ukrainian army this number is incorrect and that losses in

artillery weapons "were way below those reported" and that these losses "have nothing to do with the stated cause".[162]

In 2014, the Russians were suspected to use a cyber weapon called "Snake", or "Ouroboros," to conduct a cyber attack on Ukraine during a period of political turmoil. The Snake tool kit began spreading into Ukrainian computer systems in 2010. It performed Computer Network Exploitation (CNE), as well as highly sophisticated Computer Network Attacks (CNA).[163]

On 23 December 2015 the Black-Energy malware was used in a cyberattack on Ukraine's power-grid that left more than 200,000 people temporarily without power. A mining company and a large railway operator were also victims of the attack.[164]

Ukraine saw a massive surge in cyber attacks during the 2022 Russian invasion of Ukraine. Several websites belonging to Ukrainian banks and government departments became inaccessible.[165]

United Kingdom

MI6 reportedly infiltrated an Al Qaeda website and replaced the instructions for making a pipe bomb with the recipe for making cupcakes.[166]

In October 2010, Iain Lobban, the director of the Government Communications Headquarters (GCHQ), said the UK faces a "real and credible" threat from cyber attacks by hostile states and criminals and government systems are targeted 1,000 times each month, such attacks threatened the UK's economic future, and some countries were already using cyber assaults to put pressure on other nations.[167]

On 12 November 2013, financial organizations in London conducted cyber war games dubbed "Waking Shark 2"[168] to simulate massive internet-based attacks against bank and other financial organizations. The Waking Shark 2 cyber war games followed a similar exercise in Wall Street.[169]

Middle East

Iran

Iran has been both victim and perpetrator of several cyberwarfare operations. Iran is considered an emerging military power in the field.[170]

Flag of Cyber Police (FATA) of Islamic Republic of Iran

In September 2010, Iran was attacked by the Stuxnet worm, thought to specifically target its Natanz nuclear enrichment facility. It was a 500-kilobyte computer worm that infected at least 14 industrial sites in Iran, including the Natanz uranium-enrichment plant. Although the official authors of Stuxnet haven't been officially identified, Stuxnet is believed to be developed and deployed by the United States and Israel.[171] The worm is said to be the most advanced piece of malware ever discovered and significantly increases the profile of cyberwarfare.[172][173]

Iranian Cyber Police department, FATA, was dismissed one year after its creation in 2011 because of the arrest and death of Sattar Behesti, a blogger, in the custody of FATA. Since then, the main responsible institution for the cyberwarfare in Iran is the "Cyber Defense Command" operating under the Joint Staff of Iranian Armed Forces.

Israel

In the 2006 war against Hezbollah, Israel alleges that cyber-warfare was part of the conflict, where the Israel Defense Forces (IDF) intelligence estimates several countries in the Middle East used Russian hackers and scientists to operate on their behalf. As a result, Israel attached growing importance to cyber-tactics, and became, along with the U.S., France and a couple of other nations, involved in cyber-war planning. Many international high-tech companies are now locating research and development operations in Israel, where local hires are often veterans of the IDF's elite computer units.[174] Richard A. Clarke adds that "our Israeli friends have learned a thing or two from the programs we have been working on for more than two decades."[14]:8

In September 2007, Israel carried out an airstrike on a suspected nuclear reactor[175] in Syria dubbed Operation Orchard. U.S. industry and military sources speculated that the Israelis may have used cyberwarfare to allow their planes to pass undetected by radar into Syria.[176][177]

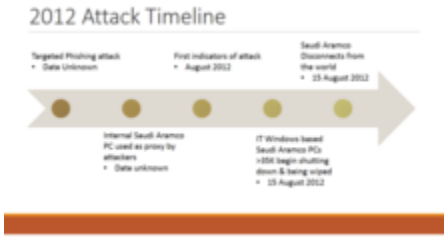
Following US President Donald Trump's decision to pull out of the Iran nuclear deal in May 2018, cyber warfare units in the United States and Israel monitoring internet traffic out of Iran noted a surge in retaliatory cyber attacks from Iran. Security firms warned that Iranian hackers were sending emails containing malware to diplomats who work in the foreign affairs offices of US allies and employees at telecommunications companies, trying to infiltrate their computer systems.[178]

Saudi Arabia

On 15 August 2012 at 11:08 am local time, the Shamoon virus began destroying over 35,000 computer systems, rendering them inoperable. The virus used to target the Saudi government by causing destruction to the state owned national oil company Saudi Aramco. The attackers posted a pastie on PasteBin.com hours prior to the wiper logic bomb occurring, citing oppression and the Al-Saud regime as a reason behind the attack.[179]

Pastie announcing attack against Saudi Aramco by a group called Cutting Sword of Justice

The attack was well staged according to Chris Kubecka, a former security advisor to Saudi Aramco after the attack and group leader of security for Aramco Overseas.[180] It was an unnamed Saudi Aramco employee on the Information Technology team which opened a malicious phishing email, allowing initial entry into the computer network around mid-2012.[181]



Shamoon 1 attack timeline against Saudi Aramco

Kubecka also detailed in her Black Hat USA talk Saudi Aramco placed the majority of their security budget on the ICS control network, leaving the business network at risk for a major incident. "When you realize most of your security budget was spent on ICS & IT gets Pwnd".[181] The virus has been noted to have behavior differing from other malware attacks, due to the destructive nature and the cost of the attack and recovery. US Defense Secretary Leon Panetta called the attack a "Cyber Pearl Harbor"[182] Known years later as the "Biggest hack in history" and intended for cyber warfare.[183] Shamoon can spread from an infected machine to other computers on the network. Once a system is infected, the virus continues to compile a list of files from specific locations on the system, upload them to the attacker, and erase them. Finally the virus overwrites the master boot record of the infected computer, making it unusable.[184][185] The virus has been used for cyber warfare against the national oil companies Saudi Aramco and Qatar's RasGas.[186][187][184][188]

Saudi Aramco announced the attack on their Facebook page and went offline again until a company statement was issued on 25 August 2012. The statement falsely reported normal business was resumed on 25 August 2012. However a Middle Eastern journalist leaked photographs taken on 1 September 2012 showing kilometers of petrol trucks unable to be loaded due to backed business systems still inoperable.

Tanker trucks unable to be loaded with gasoline due to Shamoon attacks

On 29 August 2012 the same attackers behind Shamoon posted another pastie on PasteBin.com, taunting Saudi Aramco with proof they still retained access to the company network. The post contained the username and password on security and network equipment and the new password for the CEO Khalid Al- Falih[189] The attackers also referenced a portion of the Shamoon malware as further proof in the pastie.

According to Kubecka, in order to restore operations. Saudi Aramco used its large private fleet of aircraft and available funds to purchase much of the world's hard drives, driving the price up. New hard drives were required as quickly as possible so oil prices were not affected by speculation. By 1 September 2012 gasoline resources were dwindling for the public of Saudi Arabia 17 days after the 15 August attack. RasGas was also affected by a different variant, crippling them in a similar manner.[190]

Qatar

In March 2018 American Republican fundraiser Elliott Broidy filed a lawsuit against Qatar, alleging that Qatar's government stole and leaked his emails in order to discredit him because he was viewed "as an impediment to their plan to improve the country's standing in Washington."[191] In May 2018, the lawsuit named Mohammed bin Hamad bin Khalifa Al Thani, brother of the Emir of Qatar, and his associate Ahmed Al-Rumaihi, as allegedly orchestrating Qatar's cyber warfare campaign against Broidy.[192] Further litigation revealed that the same cybercriminals who targeted Broidy had targeted as many as 1,200 other individuals, some of whom are also "well-known enemies of Qatar" such as senior officials of the U.A.E., Egypt, Saudi Arabia, and Bahrain. While these hackers almost always obscured their location, some of their activity was traced to a telecommunication network in Qatar.[193]

United Arab Emirates

The United Arab Emirates has launched several cyber-attacks in the past targeting dissidents. Ahmed Mansoor, an Emirati citizen, was jailed for sharing his thoughts on Facebook and Twitter.[194] He was given the code name Egret under the state-led covert project called Raven,

which spied on top political opponents, dissidents, and journalists. Project Raven deployed a secret hacking tool called Karma, to spy without requiring the target to engage with any web links.[195]

In September 2021, three of the former American intelligence officers, Marc Baier, Ryan Adams, and Daniel Gericke, admitted to assisting the UAE in hacking crimes by providing them with advanced technology and violating US laws. Under a three-year deferred prosecution agreement with the Justice Department, the three defendants also agreed to pay nearly $1.7 million in fines to evade prison sentences. The court documents revealed that the Emirates hacked into the computers and mobile phones of dissidents, activists, and journalists. They also attempted to break into the systems of the US and rest of the world.[196]

North America

United States

Cyberwarfare in the United States is a part of the American military strategy of proactive cyber defence and the use of cyberwarfare as a platform for attack.[197] The new United States military strategy makes explicit that a cyberattack is *casus belli* just as a traditional act of war.[198]

U.S. government security expert Richard A. Clarke, in his book *Cyber War* (May 2010), had defined "cyberwarfare" as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[14]:6 *The Economist* describes cyberspace as "the fifth domain of warfare,"[199] and William J. Lynn, U.S. Deputy Secretary of Defense, states that "as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare . . . [which] has become just as critical to military operations as land, sea, air, and space."[200]

In 2009, president Barack Obama declared America's digital infrastructure to be a "strategic national asset," and in May 2010 the Pentagon set up its new U.S. Cyber Command (USCYBERCOM), headed by General Keith B. Alexander, director of the National Security Agency (NSA), to defend American military networks and attack other countries' systems. The EU has set up ENISA (European Union Agency for Network and Information Security) which is headed by Prof. Udo Helmbrecht and there are now further plans to significantly expand ENISA's capabilities. The United Kingdom has also set up a cyber-security and "operations centre" based in Government Communications Headquarters (GCHQ), the British equivalent of the NSA. In the U.S. however, Cyber Command is only set up to protect the military, whereas the government and

corporate infrastructures are primarily the responsibility respectively of the Department of Homeland Security and private companies.[199]

In February 2010, top American lawmakers warned that the "threat of a crippling attack on telecommunications and computer networks was sharply on the rise."[201] According to The Lipman Report, numerous key sectors of the U.S. economy along with that of other nations, are currently at risk, including cyber threats to public and private facilities, banking and finance, transportation, manufacturing, medical, education and government, all of which are now dependent on computers for daily operations.[201] In 2009, president Obama stated that "cyber intruders have probed our electrical grids."[202]

On 19 June 2010, United States Senator Joe Lieberman (I-CT) introduced a bill called "Protecting Cyberspace as a National Asset Act of 2010",[203] which he co-wrote with Senator Susan Collins (R-ME) and Senator Thomas Carper (D-DE). If signed into law, this controversial bill, which the American media dubbed the "*Kill switch bill*", would grant the president emergency powers over parts of the Internet. However, all three co-authors of the bill issued a statement that instead, the bill "[narrowed] existing broad presidential authority to take over telecommunications networks".[204] In June 2012 *the New York Times* reported that president Obama had ordered the cyber attack on Iranian nuclear enrichment facilities.[205]

In July 2010, *The Economist* wrote that China had plans of "winning informationised wars by the mid-21st century", that other countries were likewise organizing for cyberwar, among them Russia, Israel and North Korea, and that Iran boasted of having the world's second-largest cyber-army.[199] James Gosler, a government cybersecurity specialist, worried that the U.S. has a severe shortage of computer security specialists, estimating that there are only about 1,000 qualified people in the country today, but needs a force of 20,000 to 30,000 skilled experts.[206] At the July 2010 Black Hat computer security conference, Michael Hayden, former deputy director of national intelligence, challenged thousands of attendees to help devise ways to "reshape the Internet's security architecture", explaining, "You guys made the cyberworld look like the north German plain."[207]

In August 2010, the U.S. for the first time warned publicly about the Chinese military's use of civilian computer experts in clandestine cyber attacks aimed at American companies and government agencies. The Pentagon also pointed to an alleged China-based computer spying network dubbed GhostNet which was revealed in a 2009 research report.[208] The Pentagon stated:

> The People's Liberation Army is using "information warfare units" to develop viruses to attack enemy computer systems and networks, and those units include civilian computer professionals. Commander Bob Mehal, will monitor the PLA's buildup of its cyberwarfare capabilities and will continue to develop capabilities to counter any potential threat.[209]

United States Department of Defense Seal

The United States Department of Defense sees the use of computers and the Internet to conduct warfare in cyberspace as a threat to national security. The United States Joint Forces Command describes some of its attributes:

> Cyberspace technology is emerging as an "instrument of power" in societies, and is becoming more available to a country's opponents, who may use it to attack, degrade, and disrupt communications and the flow of information. With low barriers to entry, coupled with the anonymous nature of activities in cyberspace, the list of potential adversaries is broad. Furthermore, the globe-spanning range of cyberspace and its disregard for national borders will challenge legal systems and complicate a nation's ability to deter threats and respond to contingencies.[210]

Seal of Joint Force Headquarters Cyber Air Force

In February 2010, the United States Joint Forces Command released a study which included a summary of the threats posed by the internet:[210]

> With very little investment, and cloaked in a veil of anonymity, our adversaries will inevitably attempt to harm our national interests. Cyberspace will become a main front in both irregular and traditional conflicts. Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In much the same way that airpower transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication. Indeed, adversaries have already taken advantage of computer networks and the power of information technology not only to plan and execute savage acts of terrorism, but also to influence directly the perceptions and will of the U.S. Government and the American population.

On 6 October 2011, it was announced that Creech AFB's drone and Predator fleet's command and control data stream had been keylogged, resisting all attempts to reverse the exploit, for the past two weeks.[211] The Air Force issued a statement that the virus had "posed no threat to our operational mission".[212]

On 21 November 2011, it was widely reported in the U.S. media that a hacker had destroyed a water pump at the Curran-Gardner Township Public Water District in Illinois.[213] However, it later turned out that this information was not only false, but had been inappropriately leaked from the Illinois Statewide Terrorism and Intelligence Center.[214]

In 2012, the US used cyberattacks for tactical advantage in Afghanistan.[215]

According to a 2013 *Foreign Policy* magazine article, NSA's Tailored Access Operations (TAO) unit "has successfully penetrated Chinese computer and telecommunications systems for almost 15 years, generating some of the best and most reliable intelligence information about what is going on inside the People's Republic of China."[216][217]

In 2013 cyberwarfare was, for the first time, considered a larger threat than Al Qaeda or terrorism, by many U.S. intelligence officials.[218] In 2017, Representative Mike Rogers, chairman of the U.S. House Permanent Select Committee on Intelligence, for instance, said that "We are in a cyber war in this country, and most Americans don't know it. And we are not necessarily winning. We have got huge challenges when it comes to cybersecurity."[219]

In 2014, Barack Obama ordered an intensification of cyberwarfare against North Korea's missile program for sabotaging test launches in their opening seconds.[220] On 24 November 2014, Sony Pictures Entertainment hack was a release of confidential data belonging to Sony Pictures Entertainment (SPE).

In June 2015, the United States Office of Personnel Management (OPM) announced that it had been the target of a data breach targeting the records of as many as four million people.[221] Later, FBI Director James Comey put the number at 18 million.[222] The *Washington Post* has reported that the attack originated in China, citing unnamed government officials.[223]

In October 2016, Jeh Johnson the United States Secretary of Homeland Security and James Clapper the U.S. Director of National Intelligence issued a joint statement accusing Russia of interfering with the 2016 United States presidential election.[224] The New York Times reported the Obama administration formally accused Russia of stealing and disclosing Democratic National Committee emails.[225] Under U.S. law (50 U.S.C.Title 50 – War and National Defense,

Chapter 15 – National Security, Subchapter III Accountability for Intelligence Activities[226]) there must be a formal *Presidential finding* prior to authorizing a covert attack. Then U.S. vice president Joe Biden said on the American news interview program *Meet The Press* that the United States will respond.[227] The New York Times noted that Biden's comment "seems to suggest that Mr. Obama is prepared to order – or has already ordered – some kind of covert action".[228] In 2016 President Barack Obama authorized the planting of cyber weapons in Russian infrastructure in the final weeks of his presidency in response to Moscow's interference in the 2016 presidential election.[229] On 29 December 2016 United States imposed the most extensive sanctions against Russia since the Cold War,[230] expelling 35 Russian diplomats from the United States.[231][232]

Economic sanctions are the most frequently used the foreign policy instruments by the United States today[233] Thus, it is not surprising to see that economic sanctions are also used as counter policies against cyberattacks. According to Onder (2021), economic sanctions are also information gathering mechanisms for the sanctioning states about the capabilities of the sanctioned states.[234]

In March 2017, WikiLeaks published more than 8,000 documents on the CIA. The confidential documents, codenamed Vault 7 and dated from 2013 to 2016, include details on CIA's software capabilities, such as the ability to compromise cars, smart TVs,[235] web browsers (including Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera Software ASA),[236][237][238] and the operating systems of most smartphones (including Apple's iOS and Google's Android), as well as other operating systems such as Microsoft Windows, macOS, and Linux.[239]

For a global perspective of countries and other actors engaged in cyber warfare, see the George Washington University-based National Security Archive's CyberWar map.[240]

Cyberpeace

The rise of cyber as a warfighting domain has led to efforts to determine how cyberspace can be used to foster peace. For example, the German civil rights panel FIfF runs a campaign for cyberpeace – for the control of cyberweapons and surveillance technology and against the militarization of cyberspace and the development and stockpiling of offensive exploits and malware.[241][242][243][244] Measures for cyberpeace include policymakers developing new rules and norms for warfare, individuals and organizations building new tools and secure infrastructures, promoting open source, the establishment of cyber security centers, auditing of critical infrastructure cybersecurity, obligations to disclose vulnerabilities, disarmament,

defensive security strategies, decentralization, education and widely applying relevant tools and infrastructures, encryption and other cyberdefenses.[241][245][246][247]

The topics of cyber peacekeeping[248][249] and cyber peacemaking[250] have also been studied by researchers, as a way to restore and strengthen peace in the aftermath of both cyber and traditional warfare.

Cyber counterintelligence

Cyber counter-intelligence are measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.[251]

- On 7 April 2009, The Pentagon announced they spent more than $100 million in the last six months responding to and repairing damage from cyber attacks and other computer network problems.[252]
- On 1 April 2009, U.S. lawmakers pushed for the appointment of a White House cyber security "czar" to dramatically escalate U.S. defenses against cyber attacks, crafting proposals that would empower the government to set and enforce security standards for private industry for the first time.[253]
- On 9 February 2009, the White House announced that it will conduct a review of the country's cyber security to ensure that the Federal government of the United States cyber security initiatives are appropriately integrated, resourced and coordinated with the United States Congress and the private sector.[254]
- In the wake of the 2007 cyberwar waged against Estonia, NATO established the Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia, in order to enhance the organization's cyber defence capability. The center was formally established on 14 May 2008, and it received full accreditation by NATO and attained the status of International Military Organization on 28 October 2008.[255] Since Estonia has led international efforts to fight cybercrime, the United States Federal Bureau of Investigation says it will permanently base a computer crime expert in Estonia in 2009 to help fight international threats against computer systems.[256]
- In 2015, the Department of Defense released an updated cyber strategy memorandum detailing the present and future tactics deployed in the service of defense against

cyberwarfare. In this memorandum, three cybermissions are laid out. The first cybermission seeks to arm and maintain existing capabilities in the area of cyberspace, the second cybermission focuses on prevention of cyberwarfare, and the third cybermission includes strategies for retaliation and preemption (as distinguished from prevention).[257]

One of the hardest issues in cyber counterintelligence is the problem of attribution. Unlike conventional warfare, figuring out who is behind an attack can be very difficult.[258] However Defense Secretary Leon Panetta has claimed that the United States has the capability to trace attacks back to their sources and hold the attackers "accountable".[259]

Doubts about existence

In October 2011 the *Journal of Strategic Studies*, a leading journal in that field, published an article by Thomas Rid, "Cyber War Will Not Take Place" which argued that all politically motivated cyber attacks are merely sophisticated versions of sabotage, espionage, or subversion – and that it is unlikely that cyber war will occur in the future.[260]

Legal perspective

Various parties have attempted to come up with international legal frameworks to clarify what is and is not acceptable, but none have yet been widely accepted.

The Tallinn Manual, published in 2013, is an academic, non-binding study on how international law, in particular the jus ad bellum and international humanitarian law, apply to cyber conflicts and cyber warfare. It was written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence by an international group of approximately twenty experts between 2009 and 2012.

The Shanghai Cooperation Organisation (members of which include China and Russia) defines cyberwar to include dissemination of information "harmful to the spiritual, moral and cultural spheres of other states". In September 2011, these countries proposed to the UN Secretary General a document called "International code of conduct for information security".[261]

In contrast, the United approach focuses on physical and economic damage and injury, putting political concerns under freedom of speech. This difference of opinion has led to reluctance in the West to pursue global cyber arms control agreements.[262] However, American General Keith B. Alexander did endorse talks with Russia over a proposal to limit military attacks in

cyberspace.[263] In June 2013, Barack Obama and Vladimir Putin agreed to install a secure *Cyberwar-Hotline* providing "a direct secure voice communications line between the US cybersecurity coordinator and the Russian deputy secretary of the security council, should there be a need to directly manage a crisis situation arising from an ICT security incident" (White House quote).[264]

A Ukrainian professor of International Law, Alexander Merezhko, has developed a project called the International Convention on Prohibition of Cyberwar in Internet. According to this project, cyberwar is defined as the use of Internet and related technological means by one state against the political, economic, technological and information sovereignty and independence of another state. Professor Merezhko's project suggests that the Internet ought to remain free from warfare tactics and be treated as an international landmark. He states that the Internet (cyberspace) is a "common heritage of mankind".[265]

On the February 2017 RSA Conference Microsoft president Brad Smith suggested global rules – a "Digital Geneva Convention" – for cyber attacks that "ban the nation-state hacking of all the civilian aspects of our economic and political infrastructures". He also stated that an independent organization could investigate and publicly disclose evidence that attributes nation-state attacks to specific countries. Furthermore, he said that the technology sector should collectively and neutrally work together to protect Internet users and pledge to remain neutral in conflict and not aid governments in offensive activity and to adopt a coordinated disclosure process for software and hardware vulnerabilities.[266][267] A fact-binding body has also been proposed to regulate cyber operations.[268][269]

In popular culture

In films

- *Independence Day* (1996)
- *Terminator 3: Rise of the Machines* (2003)
- *Live Free or Die Hard* (2007)
- *Terminator Genisys* (2015)
- *Terminator: Dark Fate* (2019)

Documentaries

- *Hacking the Infrastructure: Cyber Warfare* (2016) by Viceland

- *Cyber War Threat* (2015)
- *Darknet, Hacker, Cyberwar*[270] (2017)
- *Zero Days* (2016)
- *The Perfect Weapon* (2020)

In television

- "Cancelled", an episode of the animated sitcom *South Park*
- Series 2 of *COBRA*, a British thriller series, revolves around a sustained campaign of cyberwar against the United Kingdom and the British government's response to it

See also

- Automated teller machine
- Computer security organizations
- Cyber spying
- Cyber-arms industry
- Cyber-collection
- Cyberterrorism
- Cyberweapon
- Duqu
- Fifth Dimension Operations
- IT risk
- iWar
- List of cyber attack threat trends
- List of cyber warfare forces
- List of cyberattacks
- Penetration test
- Proactive cyber defence
- Signals intelligence
- United States Cyber Command
  - Air Force Cyber Command
  - Fleet Cyber Command
  - Marine Corps Cyberspace Command
  - United States Army Cyber Command
- Virtual war
- Convention on Cybercrime

References

1. *Singer, P. W.; Friedman, Allan (March 2014). Cybersecurity and cyberwar : what everyone needs to know. Oxford. ISBN 9780199918096. OCLC 802324804 (https://www.worldcat.org/oclc/802324804)* .
2. *"Cyberwar - does it exist?" (https://www.nato.int/docu/review/2013/Cyber/Cyberwar-does-it-exist/EN/index.htm)* . *NATO. 13 June 2019. Retrieved 10 May 2019.*

3. *Smith, Troy E. (2013). "Cyber Warfare: A Misrepresentation of the True Cyber Threat" (https://www.jstor.org/stable/26202046) . American Intelligence Journal. **31** (1): 82–85. ISSN 0883-072X (https://www.worldcat.org/issn/0883-072X) . JSTOR 26202046 (https://www.jstor.org/stable/26202046) .*
4. *Lucas, George (2017). Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. Oxford. p. 6. ISBN 9780190276522.*
5. *"Advanced Persistent Threat Groups" (https://www.fireeye.com/current-threats/apt-groups.html) . FireEye. Retrieved 10 May 2019.*
6. *"APT trends report Q1 2019" (https://securelist.com/apt-trends-report-q1-2019/90643/) . securelist.com. Retrieved 10 May 2019.*
7. *"GCHQ" (https://www.gchq.gov.uk/news/the-uk-is-a-global-cyber-power--says-director-gchq) . www.gchq.gov.uk. Retrieved 10 May 2019.*
8. *"Who are the cyberwar superpowers?" (https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/) . World Economic Forum. Retrieved 24 June 2021.*
9. *Cyber warfare : a multidisciplinary analysis. Green, James A., 1981-. London. 7 November 2016. ISBN 9780415787079. OCLC 980939904 (https://www.worldcat.org/oclc/980939904) .*
10. *Newman, Lily Hay (6 May 2019). "What Israel's Strike on Hamas Hackers Means For Cyberwar" (https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/) . Wired. ISSN 1059-1028 (https://www.worldcat.org/issn/1059-1028) . Retrieved 10 May 2019.*
11. *Liptak, Andrew (5 May 2019). "Israel launched an airstrike in response to a Hamas cyberattack" (https://www.theverge.com/2019/5/5/18530412/israel-defense-force-hamas-cyber-attack-air-strike) . The Verge. Retrieved 10 May 2019.*
12. *Robinson, Michael; Jones, Kevin; Helge, Janicke (2015). "Cyber Warfare Issues and Challenges" (https://www.researchgate.net/publication/276248097) . Computers and Security. **49**: 70–94. doi:10.1016/j.cose.2014.11.007 (https://doi.org/10.1016%2Fj.cose.2014.11.007) . Retrieved 7 January 2020.*
13. *Shakarian, Paulo (2013). Introduction to cyber-warfare : a multidisciplinary approach. Shakarian, Jana., Ruef, Andrew. Amsterdam [Netherlands]: Morgan Kaufmann Publishers, an imprint of Elsevier. ISBN 9780124079267. OCLC 846492852 (https://www.worldcat.org/oclc/846492852) .*
14. *Clarke, Richard A. Cyber War, HarperCollins (2010) ISBN 9780061962233*

15. *Blitz, James (1 November 2011). "Security: A huge challenge from China, Russia and organised crime" (https://web.archive.org/web/20150606203810/http://www.paconsulting.com/introducing-pas-media-site/highlighting-pas-expertise-in-the-media/articles-quoting-pa-experts/financial-times-security-a-huge-challenge-from-china-russia-and-organised-crime-1-november-2011/) . Financial Times. Archived from the original (http://www.paconsulting.com/introducing-pas-media-site/highlighting-pas-expertise-in-the-media/articles-quoting-pa-experts/financial-times-security-a-huge-challenge-from-china-russia-and-organised-crime-1-november-2011/) on 6 June 2015. Retrieved 6 June 2015.*

16. *Arquilla, John (1999). "Can information warfare ever be just?" (http://philpapers.org/rec/ARQCIW) . Ethics and Information Technology. **1** (3): 203–212. doi:10.1023/A:1010066528521 (https://doi.org/10.1023%2FA%3A1010066528521) . S2CID 29263858 (https://api.semanticscholar.org/CorpusID:29263858) .*

17. *Parks, Raymond C.; Duggan, David P. (September 2011). "Principles of Cyberwarfare" (https://ieeexplore.ieee.org/document/6029360) . IEEE Security Privacy. **9** (5): 30–35. doi:10.1109/MSP.2011.138 (https://doi.org/10.1109%2FMSP.2011.138) . ISSN 1558-4046 (https://www.worldcat.org/issn/1558-4046) . S2CID 17374534 (https://api.semanticscholar.org/CorpusID:17374534) .*

18. *Taddeo, Mariarosaria (19 July 2012). An analysis for a just cyber warfare (https://ieeexplore.ieee.org/document/6243976) . Cyber Conflict (ICCC), International Conference on. Estonia: IEEE.*

19. *"Implications of Privacy & Security Research for the Upcoming Battlefield of Things | Journal of Information Warfare" (https://www.jinfowar.com/journal/volume-17-issue-4/implications-privacy-security-research-upcoming-battlefield-things) . www.jinfowar.com. Retrieved 6 December 2019.*

20. *"Latest viruses could mean 'end of world as we know it,' says man who discovered Flame" (http://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/) , The Times of Israel, 6 June 2012*

21. *"White House Cyber Czar: 'There Is No Cyberwar'" (https://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/) . Wired, 4 March 2010*

22. *Deibert, Ron (2011). "Tracking the emerging arms race in cyberspace" (http://bos.sagepub.com/content/67/1/1) . Bulletin of the Atomic Scientists. **67** (1): 1–8. doi:10.1177/0096340210393703 (https://doi.org/10.1177%2F0096340210393703) . S2CID 218770788 (https://api.semanticscholar.org/CorpusID:218770788) .*

23. *Kello, Lucas (2017). The Virtual Weapon and International Order (https://yalebooks.yale.edu/book/9780300220230/virtual-weapon-and-international-order) . New Haven, Conn.: Yale University Press. pp. 77–79. ISBN 9780300220230.*

24. *"The Politics of Cyberspace: Grasping the Danger" (https://www.economist.com/news/books-and-arts/21727048-academia-still-grappling-problems-beset-computers-and-networks) . The Economist. London. 26 August 2017.*

25. *"The Characterization and Conditions of the Gray Zone" (http://nsiteam.com/social/wp-content/uploads/2017/01/Final_NSI-ViTTa-Analysis_The-Characterization-and-Conditions-of-the-Gray-Zone.pdf)* (PDF). *Archived (https://web.archive.org/web/20210905011953/http://nsiteam.com/social/wp-content/uploads/2017/01/Final_NSI-ViTTa-Analysis_The-Characterization-and-Conditions-of-the-Gray-Zone.pdf)* (PDF) from the original on 5 September 2021.

26. *"US 'launched cyber-attack on Iran weapons systems' " (https://www.bbc.com/news/world-us-canada-48735097)* . 23 June 2019. Retrieved 9 August 2019.

27. Barnes, Julian E.; Gibbons-Neff, Thomas (22 June 2019). *"U.S. Carried Out Cyberattacks on Iran" (https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html)* . The New York Times. *ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331)* . Retrieved 9 August 2019.

28. *"Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" " (https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m)* . whitehouse.gov. 1 April 2015. Retrieved 19 June 2021.

29. *"Sanctions Programs and Country Information | U.S. Department of the Treasury" (https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information)* . home.treasury.gov. Retrieved 19 June 2021.

30. *"Cyber Sanctions" (https://www.state.gov/cyber-sanctions/)* . United States Department of State. Retrieved 19 June 2021.

31. Ratcliffe, John (18 May 2016). *"Text - H.R.5222 - 114th Congress (2015-2016): Iran Cyber Sanctions Act of 2016" (https://www.congress.gov/bill/114th-congress/house-bill/5222/text)* . www.congress.gov. Retrieved 19 June 2021.

32. Weinberger, Sharon (4 October 2007). *"How Israel Spoofed Syria's Air Defense System" (https://www.wired.com/2007/10/how-israel-spoo/)* . Wired.

33. *"Cyber espionage bug attacking Middle East, but Israel untouched — so far" (http://www.timesofisrael.com/new-cyber-bug-targeting-middle-east-but-israel-untouched-so-far/)* , The Times of Israel, 4 June 2013

34. *"A Note on the Laws of War in Cyberspace" (http://csis.org/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf)* , James A. Lewis, April 2010

35. *"Cyberwarfare" (https://www.nytimes.com/topic/subject/cyberwarfare)* . The New York Times. *ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331)* . Retrieved 21 March 2021.

36. Rayman, Noah (18 December 2013). *"Merkel Compared NSA To Stasi in Complaint To Obama" (http://world.time.com/2013/12/18/nsa-leaks-germany-merkel-obama-stasi/)* . Time. Retrieved 1 February 2014.

37. *Devereaux, Ryan; Greenwald, Glenn; Poitras, Laura (19 May 2014). "Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas" (https://web.archive.org/web/20140521045928/https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/) . The Intercept. First Look Media. Archived from the original (https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/) on 21 May 2014. Retrieved 21 May 2014.*

38. *Schonfeld, Zach (23 May 2014). "The Intercept Wouldn't Reveal a Country the U.S. Is Spying On, So WikiLeaks Did Instead" (http://www.newsweek.com/intercept-wouldnt-reveal-country-us-spying-so-wikileaks-did-instead-252320) . Newsweek. Retrieved 26 May 2014.*

39. *Bodmer, Kilger, Carpenter, & Jones (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. New York: McGraw-Hill Osborne Media. ISBN 0071772499, ISBN 978-0071772495*

40. *Sanders, Sam (4 June 2015). "Massive Data Breach Puts 4 Million Federal Employees' Records at Risk" (https://www.npr.org/sections/thetwo-way/2015/06/04/412086068/massive-data-breach-puts-4-million-federal-employees-records-at-risk) . NPR. Retrieved 5 June 2015.*

41. *Liptak, Kevin (4 June 2015). "U.S. government hacked; feds think China is the culprit" (http://www.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/) . CNN. Retrieved 5 June 2015.*

42. *Liptak, Kevin (20 June 2015). "Hacking Diplomatic Cables Is Expected. Exposing Them Is Not" (https://www.wired.com/story/eu-diplomatic-cable-hacks-area-one/) . Wired. Retrieved 22 June 2019.*

43. *"Clarke: More defense needed in cyberspace" (http://www.hometownannapolis.com/news/top/2010/09/24-11/Clarke-More-defense-needed-in-cyberspace.html) HometownAnnapolis.com, 24 September 2010*

44. *"Malware Hits Computerized Industrial Equipment" (http://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/) . The New York Times, 24 September 2010*

45. *Singer, P.W.; Friedman, Allan (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press. p. 156. ISBN 978-0-19-991809-6.*

46. *Gross, Michael L.; Canetti, Daphna; Vashdi, Dana R. (2016). "The psychological effects of cyber terrorism" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5370589) . The Bulletin of the Atomic Scientists. **72** (5): 284–291. Bibcode:2016BuAtS..72e.284G (https://ui.adsabs.harvard.edu/abs/2016BuAtS..72e.284G) . doi:10.1080/00963402.2016.1216502 (https://doi.org/10.1080%2F00963402.2016.1216502) . ISSN 0096-3402 (https://www.worldcat.org/issn/0096-3402) . PMC 5370589 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5370589) . PMID 28366962 (https://pubmed.ncbi.nlm.nih.gov/28366962) .*

47. *"Understanding Denial-of-Service Attacks | CISA" (https://us-cert.cisa.gov/ncas/tips/ST04-015) . us-cert.cisa.gov. Retrieved 10 October 2020.*

48. *Shiels, Maggie. (9 April 2009) BBC: Spies 'infiltrate US power grid' (http://news.bbc.co.uk/2/hi/technology/7990997.stm) . BBC News. Retrieved 8 November 2011.*

49. *Meserve, Jeanne (8 April 2009). "Hackers reportedly have embedded code in power grid" (http://www.cnn.com/2009/TECH/04/08/grid.threat/index.html?iref=newssearch#cnnSTCVideo) . CNN. Retrieved 8 November 2011.*

50. *"US concerned power grid vulnerable to cyber-attack" (http://in.reuters.com/article/oilRpt/idINN0853911920090408) . In.reuters.com (9 April 2009). Retrieved 8 November 2011.*

51. *Gorman, Siobhan. (8 April 2009) Electricity Grid in U.S. Penetrated By Spies (https://www.wsj.com/articles/SB123914805204099085) . The Wall Street Journal. Retrieved 8 November 2011.*

52. *NERC Public Notice (https://www.wsj.com/public/resources/documents/CIP-002-Identification-Letter-040609.pdf) . (PDF). Retrieved 8 November 2011.*

53. *Xinhua: China denies intruding into the U.S. electrical grid (https://web.archive.org/web/20090412131516/http://news.xinhuanet.com/english/2009-04/09/content_11157765.htm) . 9 April 2009*

54. *ABC News: Video (https://abcnews.go.com/Video/playerIndex?id=7286823) . ABC News. (20 April 2009). Retrieved 8 November 2011.*

55. *Micah Halpern (22 April 2015). "Iran Flexes Its Power by Transporting Turkey to the Stone Age" (https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/) . Observer.*

56. *"How Not To Prevent a Cyberwar With Russia" (https://www.wired.com/story/russia-cyberwar-escalation-power-grid/) . Wired. 18 June 2019.*

57. *"Russian military admits significant cyber-war effort" (https://www.bbc.com/news/world-europe-39062663) . bbc.com. 21 February 2017.*

58. *Ajir, Media; Vailliant, Bethany (2018). "Russian Information Warfare: Implications for Deterrence Theory" (https://www.jstor.org/stable/26481910) . Strategic Studies Quarterly. **12** (3): 70–89. ISSN 1936-1815 (https://www.worldcat.org/issn/1936-1815) . JSTOR 26481910 (https://www.jstor.org/stable/26481910) .*

59. *Carter, Nicholas (22 January 2018). "Dynamic Security Threats and the British Army" (https://web.archive.org/web/20180329141808/https://rusi.org/event/dynamic-security-threats-and-british-army) . RUSI. Archived from the original (https://rusi.org/event/dynamic-security-threats-and-british-army) on 29 March 2018. Retrieved 30 January 2018.*

60. *Cowen, Tyler (2006). "Terrorism as Theater: Analysis and Policy Implications" (https://www.jstor.org/stable/30026642) . Public Choice. **128** (1/2): 233–244. doi:10.1007/s11127-006-9051-y (https://doi.org/10.1007%2Fs11127-006-9051-y) . ISSN 0048-5829 (https://www.worldcat.org/issn/0048-5829) . JSTOR 30026642 (https://www.jstor.org/stable/30026642) . S2CID 155001568 (https://api.semanticscholar.org/CorpusID:155001568) .*

61. *"NotPetya: virus behind global attack 'masquerades' as ransomware but could be more dangerous, researchers warn" (https://web.archive.org/web/20200919091402/https://tech.newstatesman.com/security/notpetya-global-ransomware-attack-kaspersky-ransomware)* . *28 June 2017. Archived from the original (https://tech.newstatesman.com/security/notpetya-global-ransomware-attack-kaspersky-ransomware)* *on 19 September 2020. Retrieved 11 August 2020.*

62. *"NotPetya ransomware outbreak cost Merck more than $300M per quarter" (https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/)* . *TechRepublic. Retrieved 11 July 2018.*

63. *"Cyberattack Hits Ukraine Then Spreads Internationally" (https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html)* . *Retrieved 11 July 2018.*

64. *Palmer, Robert Kenneth. "Critical Infrastructure: Legislative Factors for Preventing a Cyber-Pearl Harbor." Va. JL & Tech. 18 (2013): 289.*

65. *Molfino, Emily (2012). "Viewpoint: Cyberterrorism: Cyber "Pearl Harbor" is Imminent" (https://www.routledge.com/products/isbn/9781409427544)* . *In Sean S. Costigan; Jake Perry (eds.). Cyberspaces and Global Affairs. Routledge. p. 75. ISBN 978-1-4094-2754-4.*

66. *Smith, Sean W., and John S. Erickson. "Never Mind Pearl Harbor--What about a Cyber Love Canal?." IEEE Security & Privacy 13.2 (2015): 94-98.*

67. *Loui, Ronald P., and Terrence D. Loui. "How to Survive a Cyber Pearl Harbor." Computer 49.6 (2016): 31-37.*

68. *Wirtz, James J. "The Cyber Pearl Harbor." Intelligence and National Security (2017): 1-10.*

69. *Arquilla, John (27 July 2009). "Click, click... counting down to cyber 9/11" (https://covertress.blogspot.com/2009/07/click-click-counting-down-to-cyber-911.html)* . *SFGate. Archived (https://web.archive.org/web/20120301195811/https://covertress.blogspot.com/2009/07/click-click-counting-down-to-cyber-911.html)* *from the original on 1 March 2012. Retrieved 15 May 2019. (Link (https://www.sfgate.com/opinion/article/Click-click-hellip-counting-down-to-Cyber-9-11-3291819.php)* *at SFGate)*

70. *Magee, Clifford S. (Marine Corps Command and Staff College. Quantico VA) (Third Quarter 2013). "Awaiting the Cyber 9/11" (https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ-70_76-82_Magee.pdf)* *(PDF). Joint Force Quarterly. NDU Press (70): 76–82.*

71. *Gaycken, Sandro (2010). "Cyberwar – Das Internet als Kriegsschauplatz" (https://www.opensourcepress.de/index.php?26&backPID=178&tt_products=313)* .

72. *"Cyber-War Nominee Sees Gaps in Law" (https://www.nytimes.com/2010/04/15/world/15military.html?nl=technology&emc=techupdateema1)* , *The New York Times, 14 April 2010*

73. *Cyber ShockWave Shows U.S. Unprepared For Cyber Threats (http://www.bipartisanpolicy.org/news/press-releases/2010/02/cyber-shockwave-shows-us-unprepared-cyber-threats) Archived (https://web.archive.org/web/20130719031036/http://bipartisanpolicy.org/news/press-releases/2010/02/cyber-shockwave-shows-us-unprepared-cyber-threats) 19 July 2013 at the Wayback Machine. Bipartisanpolicy.org. Retrieved 8 November 2011.*

74. *Drogin, Bob (17 February 2010). "In a doomsday cyber attack scenario, answers are unsettling" (https://www.latimes.com/news/nation-and-world/la-na-cyber-attack17-2010feb17,0,305928.story?track=rss) . Los Angeles Times.*

75. *Ali, Sarmad (16 February 2010). "Washington Group Tests Security in 'Cyber ShockWave' " (https://blogs.wsj.com/digits/2010/02/16/washington-group-tests-security-in-cyber-shockwave/) . The Wall Street Journal.*

76. *Cyber ShockWave CNN/BPC wargame: was it a failure? (http://blogs.computerworld.com/15603/cyber_shockwave_cnn_bpc_wargame_was_it_a_failure) Archived (https://web.archive.org/web/20100223000551/http://blogs.computerworld.com/15603/cyber_shockwave_cnn_bpc_wargame_was_it_a_failure) 23 February 2010 at the Wayback Machine. Computerworld (17 February 2010). Retrieved 8 November 2011.*

77. *Steve Ragan Report: The Cyber ShockWave event and its aftermath (http://www.thetechherald.com/article.php/201007/5245/Report-The-Cyber-ShockWave-and-its-aftermath) Archived (https://web.archive.org/web/20110722190129/http://www.thetechherald.com/article.php/201007/5245/Report-The-Cyber-ShockWave-and-its-aftermath) 22 July 2011 at the Wayback Machine. The Tech Herald. 16 February 2010*

78. *Lee, Andy (1 May 2012). "International Cyber Warfare: Limitations and Possibilities". (http://jpi.or.kr/contents/?mid=KR1612) Archived (https://web.archive.org/web/20120327144100/http://www.jpi.or.kr/contents/?mid=KR1612) 27 March 2012 at the Wayback Machine Jeju Peace Institute.*

79. *"Azerbaijani hackers broke into over 90 armenian websites – VIDEO" (https://www.azerbaycan24.com/en/azerbaijani-hackers-broke-into-over-90-armenian-websites-video/) . Azerbaycan24. 27 September 2020.*

80. *Giles, Christopher (26 October 2020). "Nagorno-Karabakh: The Armenian-Azeri 'information wars' " (https://www.bbc.com/news/world-europe-54614392) . BBC.*

81. *"Become a Naval Cyber Warfare Engineer (CWE) : Navy.com" (http://www.navy.com/careers/information-and-technology/cyber-warfare-engineer.html) . www.navy.com.*

82. *Brantly A. & Smeets M. (2020) Military Operations in Cyberspace. In: Sookermany A. (ed.) Handbook of Military Sciences. p. 1-16. Springer, Cham doi:10.1007/978-3-030-02866-4_19-1 (https://doi.org/10.1007%2F978-3-030-02866-4_19-1)*

83. *Hayden, M. (2016). Playing to the edge: American intelligence in the age of terror (p. 137). New York: Penguin Random House.*

84. *Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. Security Studies, 26(3), 452–481.*

85. *Denning, D. E. (2015). Rethinking the cyber domain and deterrence. Joint Forces Quarterly, 77, 15. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq77/jfq-77_8-15_Denning.pdf*

86. *Lin, Tom C. W. (14 April 2016). "Financial Weapons of War". Minnesota Law Review. **100**: 1377–1440. SSRN 2765010 (https://ssrn.com/abstract=2765010) .*

87. *Denning, D. E. (2008). The ethics of cyber conflict. The Handbook of Information and Computer Ethics (http://faculty.nps.edu/dedennin/publications/Ethics%20of%20Cyber%20Conflict.pdf) . 407–429.*

88. *Kenney, Michael (2015). "Cyber-Terrorism in a Post-Stuxnet World". Orbis. **59** (1): 111–128. doi:10.1016/j.orbis.2014.11.009 (https://doi.org/10.1016%2Fj.orbis.2014.11.009) .*

89. *"North Korea took $2 billion in cyberattacks to fund weapons..." (https://www.reuters.com/article/us-northkorea-cyber-un-idUSKCN1UV1ZX) Reuters. 5 August 2019. Retrieved 9 August 2019.*

90. *"North Korea 'stole $2bn via cyber-attacks' " (https://www.bbc.com/news/world-asia-49259302) . 7 August 2019. Retrieved 9 August 2019.*

91. *"Google Attack Is Tip Of Iceberg" (http://siblog.mcafee.com/cto/google-attack-is-tip-of-iceberg/) , McAfee Security Insights, 13 January 2010*

92. *hoffmacd (18 April 2010). "U.S. Needs New National Strategy in Era of Cyberaggression, UC Paper Concludes" (https://www.uc.edu/news/articles/legacy/enews/2010/04/us-needs-new-national-strategy-in-era-of-cyberaggression-uc-paper-concludes.html) . UC News. Retrieved 6 March 2022.*

93. *"Locked Shields" (https://ccdcoe.org/exercises/locked-shields/) . ccdcoe.org. Retrieved 7 August 2019.*

94. *"Agency leads NATO team in tough cyber exercise" (https://www.ncia.nato.int/NewsRoom/Pages/20190408-Lock-Shields.aspx) . www.ncia.nato.int. Retrieved 7 August 2019.*

95. *Allison, George (11 April 2019). "NATO takes part in international cyber security exercise" (https://ukdefencejournal.org.uk/nato-takes-part-in-international-cyber-security-exercise/) . UK Defence Journal. Retrieved 7 August 2019.*

96. *"CCDCOE" (https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019/) . ccdcoe.org. Retrieved 7 August 2019.*

97. *Boffey, Daniel (27 June 2019). "EU to run war games to prepare for Russian and Chinese cyber-attacks" (https://www.theguardian.com/technology/2019/jun/27/eu-war-games-prepare-russia-china-cyber-attacks) . The Guardian. ISSN 0261-3077 (https://www.worldcat.org/issn/0261-3077) . Retrieved 7 August 2019.*

98. *Wheeler, Caroline; Shipman, Tim; Hookham, Mark (7 October 2018). "UK war-games cyber attack on Moscow" (https://www.thetimes.co.uk/article/uk-war-games-cyber-attack-on-moscow-dgxz8ppv0) . The Sunday Times. ISSN 0956-1382 (https://www.worldcat.org/issn/0956-1382) . Retrieved 8 August 2019.*

99. *Detrixhe, John. "The UK is practicing cyberattacks that could black out Moscow" (https://qz.com/1416362/the-uk-war-games-cyberattacks-that-could-black-out-moscow/) . Quartz. Retrieved 8 August 2019.*

100. *Government-sponsored cyberattacks on the rise, McAfee says (http://www.networkworld.com/news/2007/112907-government-cyberattacks.html) Archived (https://web.archive.org/web/20130617091822/http://www.networkworld.com/news/2007/112907-government-cyberattacks.html) 17 June 2013 at the Wayback Machine. Network World (29 November 2007). Retrieved 8 November 2011.*

101. *"China's Hacker Army (https://foreignpolicy.com/2010/03/03/chinas-hacker-army/) ". Foreign Policy. 3 March 2010.*

102. *"US embassy cables: China uses access to Microsoft source code to help plot cyber warfare, US fears" (https://www.theguardian.com/world/us-embassy-cables-documents/214462?INTCMP=SRCH) . The Guardian. London. 4 December 2010. Retrieved 31 December 2010.*

103. *O'Flaherty, Kate. "Marriott Breach -- What Happened, How Serious Is It And Who Is Impacted?" (https://www.forbes.com/sites/kateoflahertyuk/2018/11/30/marriott-breach-what-happened-how-serious-is-it-and-who-is-impacted/) . Forbes. Retrieved 12 December 2018.*

104. *"Starwood Reservation Database Security Incident" (https://answers.kroll.com/) . answers.kroll.com. Retrieved 12 December 2018.*

105. *Sanger, David E.; Perlroth, Nicole; Thrush, Glenn; Rappeport, Alan (11 December 2018). "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing" (https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html) . The New York Times. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331) . Retrieved 12 December 2018.*

106. *"Marriott hotel cyber attack linked to Chinese spy agency" (https://www.independent.co.uk/life-style/gadgets-and-tech/marriott-cyber-attack-starwood-hotel-data-breach-china-spy-agency-guests-a8679006.html) . The Independent. 12 December 2018. Retrieved 12 December 2018.*

107. *"Marriott cyberattack traced to Chinese hackers" (https://www.axios.com/marriott-cyberattack-traced-to-chinese-hackers-d1de3246-c85b-4fd9-8bbc-f8f19846516d.html) . Axios. 12 December 2018. Retrieved 12 December 2018.*

108. *"How China will use cyber warfare to leapfrog in military competitiveness" (https://web.archive.org/web/20110310171345/http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm) . Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies. Vol. 8, no. 1 October 2008. p. 37. Archived from the original (http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm) on 10 March 2011. Retrieved 15 January 2013.*

109. *"China to make mastering cyber warfare A priority (2011)" (https://www.npr.org/2011/06/03/136912848/-china-to-make-mastering-cyber-warfare-a-priority)* . *Washington, D.C.: NPR. Retrieved 15 January 2013.*

110. *"How China will use cyber warfare to leapfrog in military competitiveness" (https://web.archive.org/web/20110310171345/http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm)* . *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies. Vol. 8, no. 1 October 2008. p. 42. Archived from the original (http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm) on 10 March 2011. Retrieved 15 January 2013.*

111. *"How China will use cyber warfare to leapfrog in military competitiveness" (https://web.archive.org/web/20110310171345/http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm)* . *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies. Vol. 8, no. 1 October 2008. p. 43. Archived from the original (http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm) on 10 March 2011. Retrieved 15 January 2013.*

112. *"Washington, Beijing in Cyber-War Standoff" (https://web.archive.org/web/20130217225811/http://au.news.yahoo.com/latest/a/-/latest/16117821/washington-beijing-in-cyber-war-standoff/)* . *Yahoo! News. 12 February 2013. Archived from the original (http://au.news.yahoo.com/latest/a/-/latest/16117821/washington-beijing-in-cyber-war-standoff/) on 17 February 2013. Retrieved 15 January 2013.*

113. *Jim Finkle (3 August 2011). "State actor seen in "enormous" range of cyber attacks" (https://www.reuters.com/article/us-cyberattacks-idUSTRE7720HU20110803)* . *Reuters. Retrieved 3 August 2011.*

114. *Hurst, Daniel; Kuo, Lily; Graham-McLay, Charlotte (14 September 2020). "Zhenhua Data leak: personal details of millions around world gathered by China tech company" (https://www.theguardian.com/world/2020/sep/14/zhenhua-data-full-list-leak-database-personal-details-millions-china-tech-company)* . *The Guardian. Retrieved 14 September 2020.*

115. *"National Enterprise Credit Information Publicity System" (http://www.gsxt.gov.cn/%7B76CEA3961EEF0244EDD864953C3380083D1A03AA5B7C734A27D65E6B4CAEEADF63444B721FEEF7B1E66E287F66DAC3323C8983264807FE733C369B1659189EE89E439E439EE89E438F528F528F528F6E8954B5C71A6C8BFD20FD20F620496AD93BB9D17877C4C874FC5549A849944911084E190027943D21C01DC01DC01D-1600314972669%7D)* . *GSXT. Retrieved 16 September 2020.*

116. *Graham, Ben (13 September 2020). "Zhenhua Data: 35,000 Aussies being spied on by China as part of 'psychological war' " (https://web.archive.org/web/20200917043528/https://www.news.com.au/technology/online/security/zhenhua-data-35000-aussies-being-spied-on-by-china-as-part-of-psychological-war/news-story/3ce5b88c00e3ae81d59976911a96319b)* . *News.com.au — Australia's Leading News Site. Archived from the original (https://www.news.com.au/technology/online/security/zhenhua-data-35000-aussies-being-spied-on-by-china-as-part-of-psychological-war/news-story/3ce5b88c00e3ae81d59976911a96319b) on 17 September 2020. Retrieved 16 September 2020.*

117. *"Beware of the bugs: Can cyber attacks on India's critical infrastructure be thwarted?" (http://businesstoday.intoday.in/story/india-cyber-security-at-risk/1/191786.html)* . *BusinessToday. Retrieved 15 January 2013.*

118. *"5 lakh cyber warriors to bolster India's e-defence" (https://web.archive.org/web/20130126024048/http://articles.timesofindia.indiatimes.com/2012-10-16/india/34498075_1_cyber-security-cyber-attacks-cyber-warfare)* . *The Times of India. India. 16 October 2012. Archived from the original (http://articles.timesofindia.indiatimes.com/2012-10-16/india/34498075_1_cyber-security-cyber-attacks-cyber-warfare) on 26 January 2013. Retrieved 18 October 2012.*

119. *"36 government sites hacked by 'Indian Cyber Army'" (http://tribune.com.pk/story/83967/36-government-websites-hacked-by-indian-cyber-army/)* . *The Express Tribune. Retrieved 8 November 2011.*

120. *"Hacked by 'Pakistan cyber army', CBI website still not restored" (http://www.ndtv.com/article/india/hacked-by-pakistan-cyber-army-cbi-website-still-not-restored-70568?cp)* . *Ndtv.com (4 December 2010). Retrieved 8 November 2011.*

121. *Pauli, Darren. "Copy paste slacker hackers pop corp locks in ode to stolen code" (https://www.theregister.co.uk/2016/07/08/copy_paste_slacker_hackers_pop_corp_locks_in_ode_to_stolen_code/)* . *The Register.*

122. *"APT Group 'Patchwork' Cuts-and-Pastes a Potent Attack" (https://threatpost.com/apt-group-patchwork-cuts-and-pastes-a-potent-attack/119081/)* . *Threatpost. 7 July 2016. Retrieved 2 January 2017.*

123. *Pandit, Rajat (16 May 2019). "Agencies take shape for special operations, space, cyber war | India News - Times of India" (https://timesofindia.indiatimes.com/india/india-begins-setting-up-new-tri-service-agencies-to-handle-special-operations-space-and-cyberspace/articleshow/69346012.cms)* . *The Times of India. Retrieved 15 July 2019.*

124. *"White paper" (https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf) (PDF). f-secure.com.*

125. *Sudworth, John. (9 July 2009) "New cyberattacks hit South Korea" (http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm)* . *BBC News. Retrieved 8 November 2011.*

126. *Williams, Martin. UK, Not North Korea, Source of DDOS Attacks, Researcher Says (https://www.pcworld.com/article/168353/uk_not_north_korea_source_of_ddos_attacks_researcher_says.html)* . *PC World.*

127. *"28c3: Security Log Visualization with a Correlation Engine" (https://www.youtube.com/watch?v=j4pF9VUdphc)* . *YouTube. 29 December 2011. Archived (https://ghostarchive.org/varchive/youtube/20211221/j4pF9VUdphc) from the original on 21 December 2021. Retrieved 4 November 2017.*

128. *"SK Hack by an Advanced Persistent Threat" (http://www.commandfive.com/papers/C5_APT_SKHack.pdf) (PDF). Command Five Pty Ltd. Retrieved 24 September 2011.*

129. *Lee, Se Young. "South Korea raises alert after hackers attack broadcasters, banks" (http://www.globalpost.com/dispatch/news/thomson-reuters/130320/south-korea-police-investigating-server-outages-at-major-tv-net) . Global Post. Retrieved 6 April 2013.*

130. *Kim, Eun-jung (April 2013). "S. Korean military to prepare with U.S. for cyber warfare scenarios" (http://english.yonhapnews.co.kr/national/2013/04/01/20/0301000000AEN20130401004000315F.HTML) . Yonhap News Agency. Retrieved 6 April 2013.*

131. *"An Egyptian cyber attack on Ethiopia by hackers is the latest strike over the Grand Dam" (https://qz.com/africa/1874343/egypt-cyber-attack-on-ethiopia-is-strike-over-the-grand-dam/) . Quartz. 27 June 2020.*

132. *"The Ethiopian-Egyptian Water War Has Begun" (https://foreignpolicy.com/2020/09/22/the-ethiopian-egyptian-water-war-has-begun/) . Foreign Policy. 22 September 2020.*

133. *David E Sanger Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran (https://www.nytimes.com/2018/12/18/us/politics/european-diplomats-cables-hacked.html) , New York Times (2018).*

134. *Lily Hay Newman, Hacking Diplomatic Cables Is Expected. Exposing Them Is Not (https://www.wired.com/story/eu-diplomatic-cable-hacks-area-one/) , Wired (2018).*

135. *Michalis Michael, Major and successful hackers' attack in Cyprus (https://balkaneu.com/major-and-successful-hackers-attack-in-cyprus/) , BalkanEU (2019).*

136. *"War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?" (http://www.economist.com/node/16478792) . The Economist. 1 July 2010. Retrieved 2 July 2010. "Important thinking about the tactical and legal concepts of cyber-warfare is taking place in a former Soviet barracks in Estonia, now home to NATO's "centre of excellence" for cyber-defence. It was established in response to what has become known as "Web War 1", a concerted denial-of-service attack on Estonian government, media and bank web servers that was precipitated by the decision to move a Soviet-era war memorial in central Tallinn in 2007."*

137. *Estonia accuses Russia of 'cyber attack' (http://www.csmonitor.com/2007/0517/p99s01-duts.html) . The Christian Science Monitor. (17 May 2007). Retrieved 8 November 2011.*

138. *Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia" (https://www.theguardian.com/russia/article/0,,2081438,00.html) , The Guardian, 17 May 2007*

139. *Boyd, Clark. (17 June 2010) "Cyber-war a growing threat warn experts" (http://news.bbc.co.uk/2/hi/technology/10339543.stm) . BBC News. Retrieved 8 November 2011.*

140. *Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law (http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7) , 27 Berkeley J. Int'l Law. 192 (2009).*

141. *"Bienvenue sur Atlantico.fr - Atlantico.fr" (https://www.atlantico.fr/node/) . www.atlantico.fr.*

142. *"Terre, Air, Mer, Cyber ? La 4ème armée entre coup de com et réalités" (http://echoradar.eu/2014/10/13/terre-air-mer-cyber-4eme-armee-coup-com-realites/)* . *13 October 2014*.

143. *"Vers une cyber-armée française ?" (https://www.franceculture.fr/emissions/le-choix-de-la-redaction-13-14/vers-une-cyber-armee-francaise)* . *France Culture. 29 January 2013*.

144. *Nouvelle, L'Usine (13 December 2016). "Pourquoi la France se dote d'une cyber-armée - Défense" (https://www.usinenouvelle.com/article/pourquoi-la-france-se-dote-d-une-cyber-armee.N476239)* . *Usinenouvelle.com/ – via www.usinenouvelle.com*.

145. *"L'armée française consolide son commandement cyber" (https://www.lemonde.fr/international/article/2016/12/12/l-armee-francaise-consolide-son-commandement-cyber_5047780_3210.html)* . *Le Monde. 12 December 2016*.

146. *"Germany's 60-person Computer Network Operation (CNO) unit has been practicing for cyber war for years" (https://archive.today/20130615082122/http://www.acus.org/content/germanys-60-person-computer-network-operation-cno-unit-has-been-practicing-cyber-war-years)* . *Archived from the original (http://www.acus.org/content/germanys-60-person-computer-network-operation-cno-unit-has-been-practicing-cyber-war-years) on 15 June 2013*.

147. *"Hackers wanted to man front line in cyber war" (http://www.thelocal.de/sci-tech/20130324-48723.html) Archived (https://web.archive.org/web/20130529205955/http://www.thelocal.de/sci-tech/20130324-48723.html) 29 May 2013 at the Wayback Machine, The Local, 24 March 2013*

148. *"Germany to invest 100 million euros on internet surveillance: report" (http://www.inform.kz/eng/article/2567203) , Kazinform, 18 June 2013*

149. *"Greek hackers bring down over 150 Azerbaijani government websites as "support to the Armenians" " (https://greekcitytimes.com/2020/10/04/greek-hackers-bring-down-over-150-azerbaijani-government-websites-as-support-to-the-armenians/)* . *Greek City Times. 4 October 2020*.

150. *"National Cyber Security Centrum – NCSC" (http://www.ncsc.nl/)* . *14 May 2013*.

151. *"Defensie Cyber Strategie" (http://www.defensie.nl/onderwerpen/cyber-security/inhoud/defensie-cyber-strategie)* . *Retrieved 11 August 2020*.

152. *"Cyber commando" (http://www.defensie.nl/onderwerpen/cyber-security/inhoud/cyber-commando)* . *29 March 2017*.

153. *Danchev, Dancho (11 August 2008). "Coordinated Russia vs Georgia cyberattack" (http://blogs.zdnet.com/security/?p=1670)* . *ZDNet. Retrieved 25 November 2008*.

154. *Markoff, John (26 October 2009). "Old Trick Threatens the Newest Weapons (Published 2009)" (https://www.nytimes.com/2009/10/27/science/27trojan.html)* . *The New York Times. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331)* . *Retrieved 22 October 2020*.

155. *Mazanec, Brain M. (2015). The Evolution of Cyber War. USA: University of Nebraska Press. pp. 235–236. ISBN 9781612347639.*

156. *Cyberspace and the changing nature of warfare (http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-warfare/article/115929/) Archived (https://web.archive.org/web/20081203191412/http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-warfare/article/115929/) 3 December 2008 at the Wayback Machine. Strategists must be aware that part of every political and military conflict will take place on the internet, says Kenneth Geers.*

157. *"www.axisglobe.com" (https://web.archive.org/web/20160817010832/http://www.axisglobe.com/news.asp?news=14728) . Archived from the original (http://www.axisglobe.com/news.asp?news=14728) on 17 August 2016. Retrieved 1 August 2016.*

158. *Andrew Meier, Black Earth. W. W. Norton & Company, 2003, ISBN 0-393-05178-1, pages 15–16.*

159. *Ringstrom, Anna (25 January 2017). Goodman, David (ed.). "Swedish forces exposed to extensive cyber attack: Dagens Nyheter" (https://web.archive.org/web/20170125201753/https://www.reuters.com/article/us-sweden-defence-cyberattack-idUSKBN1592K2) . Reuters. Archived from the original (https://www.reuters.com/article/us-sweden-defence-cyberattack-idUSKBN1592K2) on 25 January 2017. "Sweden's armed forces were recently exposed to an extensive cyber attack that prompted them to shut down an IT system used in military exercises, daily newspaper Dagens Nyheter reported on Wednesday. The attack that affected the Caxcis IT system was confirmed to the Swedish newspaper by armed forces spokesman Philip Simon."*

160. *Ukraine's military denies Russian hack attack (https://www.yahoo.com/news/ukraines-military-denies-russian-hack-attack-143419289.html) , Yahoo! News (6 January 2017)*

161. *"Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units" (https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/) . CrowdStrike. 22 December 2016.*

162. *Defense ministry denies reports of alleged artillery losses because of Russian hackers' break into software (http://en.interfax.com.ua/news/general/395186.html) , Interfax-Ukraine (6 January 2017)*

163. *Mazanec, Brain M. (2015). The Evolution of Cyber War. USA: University of Nebraska Press. pp. 221–222. ISBN 9781612347639.*

164. *"BlackEnergy malware activity spiked in runup to Ukraine power grid takedown" (https://www.theregister.co.uk/2016/03/04/ukraine_blackenergy_confirmation/) . The Register. Retrieved 26 December 2016.*

165. *"Ukraine crisis: 'Wiper' discovered in latest cyber-attacks" (https://www.bbc.com/news/technology-60500618) . BBC News. 24 February 2022. Retrieved 24 February 2022.*

166. *"Al Qaeda rocked by apparent cyberattack. But who did it?" (http://www.csmonitor.com/USA/2012/0403/Al-Qaeda-rocked-by-apparent-cyberattack.-But-who-did-it/(page)/2) . The Chris Science Monitor. 4 April 2012.*

167. *Britain faces serious cyber threat, spy agency head warns (https://www.theglobeandmail.com/news/world/europe/britain-faces-serious-cyber-threat-spy-agency-head-warns/article1754596/) . The Globe and Mail (13 October 2010). Retrieved 8 November 2011.*

168. *"Attack the City: why the banks are 'war gaming' " (https://www.standard.co.uk/lifestyle/london-life/attack-the-city-why-the-banks-are-wargaming-an-assault-from-cyberspace-8936904.html) . 13 November 2013.*

169. *"Wall Street banks learn how to survive in staged cyber attack" (https://www.reuters.com/article/net-us-usa-banks-cyberattack-drill-idUSBRE99K06O20131021) . Reuters. 21 October 2013.*

170. *"Iran's military is preparing for cyber warfare" (http://flashcritic.com/irans-military-preparing-for-cyber-warfare/) . Flash//CRITIC Cyber Threat News. 16 September 2013. Retrieved 18 March 2015.*

171. *Denning, Dorothy E. (16 July 2012). "Stuxnet: What Has Changed?" (https://doi.org/10.3390%2Ffi4030672) . Future Internet. **4** (3): 672–687. doi:10.3390/fi4030672 (https://doi.org/10.3390%2Ffi4030672) .*

172. *AFP (1 October 2010). Stuxnet worm brings cyber warfare out of virtual world (https://www.google.com/hostednews/afp/article/ALeqM5hWP5Ga_K2k4oOosfMz39JFifrDaQ?docId=CNG.0c3a53ff7267f11501a5b3dbd9567dbf.2d1) . Google. Retrieved 8 November 2011.*

173. *Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon | Video on (http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html) . Ted.com. Retrieved 8 November 2011.*

174. *"Israel Adds Cyber-Attack to IDF" (http://www.military.com/features/0,15240,210486,00.html) , Military.com, 10 February 2010*

175. *"IAEA: Syria tried to build nuclear reactor" (https://www.ynetnews.com/articles/0,7340,L-4062001,00.html) . Ynetnews. Associated Press. 28 April 2011. Retrieved 5 March 2022.*

176. *Fulghum, David A. "Why Syria's Air Defenses Failed to Detect Israelis (http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%3a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3a2710d024-5eda-416c-b117-ae6d649146cd) ", Aviation Week & Space Technology, 3 October 2007. Retrieved 3 October 2007.*

177. *Fulghum, David A. "Israel used electronic attack in air strike against Syrian mystery target (http://www.aviationweek.com/aw/generic/story.jsp?id=news/aw100807p2.xml&headline=Israel%20used%20electronic%20attack%20in%20air%20strike%20against%20Syrian%20mystery%20target&channel=defense) ", Aviation Week & Space Technology, 8 October 2007. Retrieved 8 October 2007.*

178. *Perlroth, Nicole (12 May 2018). "Without the nuclear deal, Iranian cyber attacks resume" (https://www.smh.com.au/world/north-america/without-the-nuclear-deal-iranian-cyber-attacks-resume-20180512-p4zewk.html) . The Sydney Morning Herald.*

179. *"Pastie: 'Untitled' " (https://pastebin.com/HqAgaQRj)* . *15 August 2012. Cutting Sword of Justice. Retrieved 3 November 2017.*

180. *"Jose Pagliery:The inside story of the biggest hack in history" (https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html)* . *CNN Money. 5 August 2015. Retrieved 15 May 2019.*

181. *Christina Kubecka (29 December 2015). "How to Implement IT Security after a Cyber Meltdown" (https://www.blackhat.com/docs/us-15/materials/us-15-Kubecka-How-To-Implement-IT-Security-After-A-Cyber-Meltdown.pdf) (PDF). Retrieved 3 November 2017. (Video (https://www.youtube.com/watch?v=WyMobr_TDSI) on YouTube-archive (https://archive.org/details/youtube-WyMobr_TDSI))*

182. *"Elisabeth Bumiller and Thom Shanker: Panetta Warns of Dire Threat of Cyberattack on U.S." (https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html) 11 October 2012. Retrieved 3 November 2017.*

183. *"Exhibitionist Shamoon virus blows PCs' minds" (https://www.theregister.co.uk/2012/08/17/shamoon_malware_energy/)* . *The Register. 17 August 2012. Retrieved 3 November 2017.*

184. *"The Shamoon Attacks" (http://www.symantec.com/connect/blogs/shamoon-attacks)* . *Symantec. 16 August 2012. Retrieved 19 August 2012.*

185. *"Jose Pagliery: The inside story of the biggest hack in history" (https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html)* . *5 August 2015. Retrieved 19 August 2012.*

186. *Michael Harper (31 August 2012). "RedOrbit: Energy Company RasGas Is Infected with Shamoon Virus".*

187. *"Shamoon virus attacks Saudi oil company" (http://www.digitaljournal.com/article/331033)* . *Digital Journal. 18 August 2012. Retrieved 19 August 2012.*

188. *"Shamoon virus targets energy sector infrastructure" (https://www.bbc.co.uk/news/technology-19293797)* . *BBC News. 17 August 2012. Retrieved 19 August 2012.*

189. *"Saudi Aramco hug, another one" (https://pastebin.com/AtN7dLeW)* . *29 August 2012. Retrieved 3 November 2017.*

190. *"Youtube - Chris Kubecka: How to Implement IT Security after a Cyber Meltdown" (https://www.youtube.com/watch?v=WyMobr_TDSI)* . *YouTube. 3 August 2015. Retrieved 3 November 2017.*

191. *"GOP Fundraiser Sues Qatar Over Stolen Emails" (https://www.wsj.com/articles/gop-fundraiser-sues-qatar-over-stolen-emails-1522094870?mod=article_inline)* . *The Wall Street Journal. 26 March 2018.*

192. *"GOP Fundraiser Elliott Broidy Expands Suit Alleging Qatar-Backed Hacking" (https://www.wsj.com/articles/gop-fundraiser-elliott-broidy-expands-suit-alleging-qatar-backed-hacking-1527204900)* . *The Wall Street Journal. 25 May 2018.*

193. *"Hackers Went After a Now-Disgraced G.O.P. Fund-Raiser. Now He Is After Them" (https://www.nytimes.com/2018/09/20/world/middleeast/broidy-trump-hackers-qatar.html)* . *The New York Times. 20 September 2018.*

194. *"UAE: Activist Ahmed Mansoor sentenced to 10 years in prison for social media posts" (https://www.amnesty.org/en/latest/news/2018/05/uae-activist-ahmed-mansoor-sentenced-to-10-years-in-prison-for-social-media-posts/)* . *Amnesty International. 31 May 2018. Retrieved 31 May 2018.*

195. *"Inside the UAE's secret hacking team of American mercenaries" (https://www.reuters.com/investigates/special-report/usa-spying-raven/)* . *Reuters. Retrieved 30 January 2019.*

196. *Mazzetti, Mark; Goldman, Adam (14 September 2021). "Ex-U.S. Intelligence Officers Admit to Hacking Crimes in Work for Emiratis" (https://ghostarchive.org/archive/20211228/https://www.nytimes.com/2021/09/14/us/politics/darkmatter-uae-hacks.html?)* . *The New York Times. Archived from the original (https://www.nytimes.com/2021/09/14/us/politics/darkmatter-uae-hacks.html?)* *on 28 December 2021. Retrieved 14 September 2021.*

197. *American Forces Press Service: Lynn Explains U.S. Cybersecurity Strategy (http://www.defense.gov/news/newsarticle.aspx?id=60869)* . *Defense.gov. Retrieved 8 November 2011.*

198. *"Pentagon to Consider Cyberattacks Acts of War" (https://www.nytimes.com/2011/06/01/us/politics/01cyber.html)* . *The New York Times. 31 May 2011*

199. *"Cyberwar: War in the Fifth Domain" (http://www.economist.com/node/16481504?story_id=16481504&source=features_box1)* *Economist, 1 July 2010*

200. *Lynn, William J. III. "Defending a New Domain: The Pentagon's Cyberstrategy" (http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain)* , *Foreign Affairs, Sept/Oct. 2010, pp. 97–108*

201. *The Lipman Report (http://www.guardsmark.com/library/computer_security.asp?nav=4&subnav=1)* , *15 October 2010*

202. *Clarke, Richard. "China's Cyberassault on America" (https://www.wsj.com/articles/SB10001424052702304259304576373391101828876?mod=WSJ_hp_mostpop_read#)* , *The Wall Street Journal, 15 June 2011*

203. *A Bill. To amend the Homeland Security Act of 2002 and other laws to enhance the security and resiliency of the cyber and communications infrastructure of the United States. (http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=4ee63497-ca5b-4a4b-9bba-04b7f4cb0123)* . *Senate.gov. 111th Congress 2D Session*

204. *Senators Say Cybersecurity Bill Has No 'Kill Switch' (http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=225701368&subSection=News)* , *Information Week, 24 June 2010. Retrieved 25 June 2010.*

205. *Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." (https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1)* *The New York Times, 1 June 2012.*

206. *"Cyberwarrior Shortage Threatens U.S. Security" (https://www.npr.org/templates/story/story.php?storyId=128574055)* . *NPR, 19 July 2010*

207. *"U.S. military cyberwar: What's off-limits?" (http://news.cnet.com/8301-31921_3-20012121-281.html)* *CNET, 29 July 2010*

208. *ANNUAL REPORT TO CONGRESS Military and Security Developments Involving the People's Republic of China 2010 (http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf)* . *US Defense Department (PDF). Retrieved 8 November 2011.*

209. *"AP: Pentagon takes aim at China cyber threat" (https://web.archive.org/web/20100823023117/https://www.google.com/hostednews/ap/article/ALeqM5i49n7xcjlHBv_Uq9SOjyP7vs6f8wD9HMP8R00)* . *Archived from the original (https://www.google.com/hostednews/ap/article/ALeqM5i49n7xcjlHBv_Uq9SOjyP7vs6f8wD9HMP8R00) on 23 August 2010. Retrieved 11 August 2020.*

210. *"The Joint Operating Environment" (http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf) Archived (https://web.archive.org/web/20130810043238/http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf) 10 August 2013 at the Wayback Machine, Joint Forces Command, 18 February 2010, pp. 34–36*

211. *U.S. drone and predator fleet is being keylogged (https://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/)* . *Wired, October 2011. Retrieved 6 October 2011*

212. *Hennigan, W.J. "Air Force says drone computer virus poses 'no threat'" (http://latimesblogs.latimes.com/technology/2011/10/drone-computer-virus-air-force.html)* . *Los Angeles Times, 13 October 2011.*

213. *Mathew J. Schwartz (21 November 2011). "Hacker Apparently Triggers Illinois Water Pump Burnout" (http://www.informationweek.com/news/security/attacks/231903481)* . *InformationWeek.*

214. *Kim Zetter (30 November 2011). "Exclusive: Comedy of Errors Led to False 'Water-Pump Hack' Report" (https://www.wired.com/threatlevel/2011/11/water-pump-hack-mystery-solved/)* . *Wired.*

215. *Satter, Raphael. "US general: We hacked the enemy in Afghanistan." (http://usatoday30.usatoday.com/news/military/story/2012-08-24/afghan-cyberattack/57295168/1)* . *Associated Press, 24 August 2012.*

216. *"U.S. NSA Unit 'TAO' Hacking China For Years (http://www.businessinsider.com/us-nsa-unit-tao-hacking-china-for-years-2013-6)* *". Business Insider. 11 June 2013*

217. *"Secret NSA hackers from TAO Office have been pwning China for nearly 15 years (http://www.computerworld.com/article/2473609/cybercrime-hacking/secret-nsa-hackers-from-tao-office-have-been-pwning-china-for-nearly-15-years.html)* *". Computerworld. 11 June 2013.*

218. *Dilanian, Ken. "Cyber-attacks a bigger threat than Al Qaeda, officials say" (https://articles.latimes.com/2013/mar/12/world/la-fg-worldwide-threats-20130313)* , *Los Angeles Times, 12 March 2013*

219. *Nikita Vladimirov, Ex-House intel chairman: US 'not necessarily winning' the cyber war (http://thehill.com/policy/cybersecurity/320265-former-house-intel-chair-us-is-not-necessarily-winning-the-cyberwar) , The Hill (19 February 2017).*

220. *Sanger, David E.; Broad, William J. (4 March 2017). "Trump Inherits a Secret Cyberwar Against North Korean Missiles" (https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html) . The New York Times. Retrieved 4 March 2017.*

221. *Barrett, Devlin (5 June 2015). "U.S. Suspects Hackers in China Breached About four (4) Million People's Records, Officials Say" (https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888) . The Wall Street Journal. Retrieved 5 June 2015.*

222. *"U.S. gov't hack may be four (4) times larger than first reported" (http://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html) .*

223. *Sanders, Sam (4 June 2015). "Massive Data Breach Puts 4 Million Federal Employees' Records at Risk" (https://www.npr.org/sections/thetwo-way/2015/06/04/412086068/massive-data-breach-puts-4-million-federal-employees-records-at-risk) . NPR.*

224. *"Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security" (https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national) . Department of Homeland Security and Office of the Director of National Intelligence on Election Security. 7 October 2016. Retrieved 15 October 2016.*

225. *"U.S. Says Russia Directed Hacks to Influence Elections" (https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html?_r=0) . NYT. 7 October 2016.*

226. *"Presidential approval and reporting of covert actions" (https://www.gpo.gov/fdsys/pkg/USCODE-2009-title50/html/USCODE-2009-title50-chap15-subchapIII-sec413b.htm) . gpo.gov. United States Code. Retrieved 16 October 2016.*

227. *"VP Biden Promises Response to Russian Hacking" (http://www.nbcnews.com/meet-the-press/video/vp-biden-on-russia-and-cyber-warfare-786308675872) . NBC News Meet the Press. 14 October 2016.*

228. *"Biden Hints at U.S. Response to Russia for Cyberattacks" (https://www.nytimes.com/2016/10/16/us/politics/biden-hints-at-us-response-to-cyberattacks-blamed-on-russia.html) . NYT. 15 October 2016.*

229. *Greg Miller, Ellen Nakashima, Adam Entous: Obama's secret struggle to retaliate against Putin's election interference (https://web.archive.org/web/20170623111559/https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/) , Washington Post, 23. June 2017*

230. *Lee, Carol E.; Sonne, Paul (30 December 2016). "U.S. Sanctions Russia Over Election Hacking; Moscow Threatens to Retaliate" (https://www.wsj.com/articles/u-s-punishes-russia-over-election-hacking-with-sanctions-1483039178) . The Wall Street Journal.*

231. *"U.S. imposes sanctions on Russia over election interference" (http://www.cbsnews.com/news/us-russia-sanctions-election-interference-2016/) . CBS News. 29 December 2016. Retrieved 29 December 2016.*

232. *"US expels 35 Russian diplomats, closes two compounds: report" (http://www.dw.com/en/us-expels-35-russian-diplomats-closes-two-compounds-report/a-36947857)* . *DW.COM. 29 December 2016. Retrieved 29 December 2016.*

233. *Onder, Mehmet (2020). "Regime Type, Issue Type and Economic Sanctions: The Role of Domestic Players" (https://doi.org/10.3390%2Feconomies8010002)* . *Economies.* ***8*** *(1): 2. doi:10.3390/economies8010002 (https://doi.org/10.3390%2Feconomies8010002)* .

234. *Onder, Mehmet (2021). "Economic sanctions outcomes: An information-driven explanation" (https://www.jois.eu/files/3_1112_Onder.pdf)* *(PDF). Journal of International Studies.* ***14*** *(2): 38–57. doi:10.14254/2071-8330.2021/14-2/3 (https://doi.org/10.14254%2F2071-8330.2021%2F14-2%2F3)* . *S2CID 244621961 (https://api.semanticscholar.org/CorpusID:244621961)* *– via ProQuest.*

235. *Shane, Scott; Mazzetti, Mark; Rosenberg, Matthew (7 March 2017). "WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents" (https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html)* . *The New York Times. Retrieved 7 March 2017.*

236. *Greenberg, Andy (7 March 2017). "How the CIA Can Hack Your Phone, PC, and TV (Says WikiLeaks)" (https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/)* . *WIRED. Retrieved 8 April 2017.*

237. *Murdock, Jason (7 March 2017). "Vault 7: CIA hacking tools were used to spy on iOS, Android and Samsung smart TVs" (http://www.ibtimes.co.uk/vault-7-cia-hacking-tools-were-used-spy-ios-android-samsung-smart-tvs-1610263)* . *International Business Times UK. Retrieved 8 April 2017.*

238. *"WikiLeaks posts trove of CIA documents detailing mass hacking" (http://www.cbsnews.com/news/wikileaks-cia-documents-released-cyber-intelligence/)* . *CBS News. 7 March 2017. Retrieved 8 April 2017.*

239. *"Vault 7: Wikileaks reveals details of CIA's hacks of Android, iPhone Windows, Linux, MacOS, and even Samsung TVs (http://www.computing.co.uk/ctg/news/3006021/vault-7-wikileaks-reveals-details-of-cias-hacks-of-android-iphone-windows-linux-macos-and-even-samsung-tvs)* ". *Computing. 7 March 2017.*

240. *Michael Martelle, ed. (6 June 2018). "CyberWar Map" (https://nsarchive.gwu.edu/news/cybervault/2018-06-06/cyberwar-map)* . *National Security Archive. Retrieved 2 August 2018.*

241. *Hofkirchner, Wolfgang; Burgin, Mark (24 January 2017). The Future Information Society: Social and Technological Problems (https://books.google.com/books?id=fPmtDgAAQBAJ&pg=PA459)* . *World Scientific. ISBN 9789813108981. Retrieved 22 May 2017.*

242. *"Abrüstung statt "Cyberwar": Forderungen nach WannaCry" (https://netzpolitik.org/2017/abruestung-statt-cyberwar-forderungen-nach-wannacry/)* . *netzpolitik.org (in German). 22 May 2017. Retrieved 22 May 2017.*

243. *"WannaCry ist ein Kollateralschaden des Cyberwar – Pressenza" (https://www.pressenza.com/de/2017/05/wannacry-ist-ein-kollateralschaden-des-cyberwar/)* . *Pressenza (in German). Pressenza. 18 May 2017. Retrieved 22 May 2017.*

244. *" "Cyberpeace"-Kampagne engagierter InformatikerInnen wird gefördert" (https://www.heise.de/newsticker/meldung/Cyberpeace-Kampagne-engagierter-InformatikerInnen-wird-gefoerdert-2438720.html) . heise online (in German). Retrieved 22 May 2017.*

245. *"Eric Schmidt and Jared Cohen: We Must Prepare Ourselves for the Cyberwars of the Future" (http://time.com/4606057/cyberwars-of-the-future/) . Time. Retrieved 22 May 2017.*

246. *Friesinger, Günther; Herwig, Jana (30 June 2014). The Art of Reverse Engineering: Open – Dissect – Rebuild (https://books.google.com/books?id=8Y-TBQAAQBAJ&pg=PA149) . transcript Verlag. ISBN 9783839425039. Retrieved 22 May 2017.*

247. *Grady, Mark F.; Parisi, Francesco (28 November 2005). The Law and Economics of Cybersecurity (https://books.google.com/books?id=toLwWiJt3m0C&pg=PA283) . Cambridge University Press. ISBN 9781139446969. Retrieved 22 May 2017.*

248. *Robinson, Michael; Janicke, Helge; Jones, Kevin (2017). "An Introduction to Cyber Peacekeeping". arXiv:1710.09616 (https://arxiv.org/abs/1710.09616) [cs.CY (https://arxiv.org/archive/cs.CY)].*

249. *Akatyev, Nikolay; James, Joshua (2015). "Cyber Peacekeeping". Digital Forensics and Cyber Crime. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Vol. 157. pp. 126–139. doi:10.1007/978-3-319-25512-5_10 (https://doi.org/10.1007%2F978-3-319-25512-5_10) . ISBN 978-3-319-25511-8.*

250. *Ramsbotham, Oliver; Miall, Hugh; Woodhouse, Tom (11 April 2011). Contemporary Conflict Resolution (https://books.google.com/books?id=-IbuQE02-KkC&pg=PA365) . Polity. ISBN 9780745649740. Retrieved 22 May 2017.*

251. *DOD – Cyber Counterintelligence (https://web.archive.org/web/19970618024356/http://www.dtic.mil/doctrine/jel/doddict/data/c/01472.html) . Dtic.mil. Retrieved 8 November 2011.*

252. *Pentagon Bill To Fix Cyber Attacks: ,0M (http://www.cbsnews.com/stories/2009/04/07/tech/main4926071.shtml) . CBS News. Retrieved 8 November 2011.*

253. *"Senate Legislation Would Federalize Cybersecurity" (https://www.washingtonpost.com/wp-dyn/content/article/2009/03/31/AR2009033103684.html) . The Washington Post. Retrieved 8 November 2011.*

254. *"White House Eyes Cyber Security Plan" (http://www.cbsnews.com/blogs/2009/02/09/politics/politicalhotsheet/entry4788180.shtml) . CBS News (10 February 2009). Retrieved 8 November 2011.*

255. *CCD COE – Cyber Defence (http://www.ccdcoe.org/2.html) Archived (https://web.archive.org/web/20090531101949/http://www.ccdcoe.org/2.html) 31 May 2009 at the Wayback Machine. Ccdcoe.org. Retrieved 8 November 2011.*

256. *Associated Press (11 May 2009) FBI to station cybercrime expert in Estonia (http://www.bostonherald.com/news/international/europe/view.bg?articleid=1171516&srvc=rss) . Boston Herald. Retrieved 8 November 2011.*

257. *Lisa Lucile Owens, Justice and Warfare in Cyberspace, The Boston Review (2015), available at [1] (http://bostonreview.net/us/lisa-lucile-owens-cyber-warfare-national-security)*

258. *Reed, John. "Is the 'holy grail' of cyber security within reach?" (https://foreignpolicy.com/2012/09/06/is-the-holy-grail-of-cyber-security-within-reach/) . Foreign Policy Magazine, 6 September 2012.*

259. *Carroll, Chris. "US can trace cyberattacks, mount pre-emptive strikes, Panetta says" (http://www.stripes.com/news/us-can-trace-cyberattacks-mount-pre-emptive-strikes-panetta-says-1.192789) . Stars and Stripes, 11 October 2012.*

260. *Rid, Thomas (2012). "Cyber War Will Not Take Place". Journal of Strategic Studies. **35**: 5–32. doi:10.1080/01402390.2011.608939 (https://doi.org/10.1080%2F01402390.2011.608939) . S2CID 153828543 (https://api.semanticscholar.org/CorpusID:153828543) .*

261. *Russian Embassy to the UK [2] (http://www.rusemb.org.uk/policycontact/49) . Retrieved 25 May 2012.*

262. *Tom Gjelten (23 September 2010). "Seeing The Internet As An 'Information Weapon'" (https://www.npr.org/templates/story/story.php?storyId=130052701) . NPR. Retrieved 23 September 2010.*

263. *Gorman, Siobhan. (4 June 2010) WSJ: U.S. Backs Talks on Cyber Warfare (https://www.wsj.com/articles/SB10001424052748703340904575284964215965730?KEYWORDS=cybersecurity) . The Wall Street Journal. Retrieved 8 November 2011.*

264. *Sean Gallagher, US, Russia to install "cyber-hotline" to prevent accidental cyberwar (https://arstechnica.com/information-technology/2013/06/us-russia-to-install-cyber-hotline-to-prevent-accidental-cyberwar/) , Arstechnica, 18 June 2013*

265. *Український центр політичного менеджменту – Зміст публікації – Конвенция о запрещении использования кибервойны (http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57) Archived (https://web.archive.org/web/20111007185753/http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57) 7 October 2011 at the Wayback Machine. Politik.org.ua. Retrieved 8 November 2011.*

266. *"'Digital Geneva Convention' needed to deter nation-state hacking: Microsoft president" (https://www.reuters.com/article/us-microsoft-cyber-idUSKBN15T26V) . Reuters. 14 February 2017. Retrieved 20 February 2017.*

267. *Kaspersky, Eugene. "A Digital Geneva Convention? A Great Idea" (https://www.forbes.com/sites/eugenekaspersky/2017/02/15/a-digital-geneva-convention-a-great-idea/) . Forbes. Retrieved 20 February 2017.*

268. *"Regulating the Use and Conduct of Cyber Operations: Challenges and a Fact-Finding Body Proposal", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540615 (2019/2020)*

269. *"An International Attribution Mechanism for Hostile Cyber Operations", https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2922&context=ils*

270. *"Darknet, Hacker, Cyberwar – Der geheime Krieg im Netz" (https://web.archive.org/web/20170404053318/https://www.zdf.de/dokumentation/zdfinfo-doku/darknet-hacker-cyberwar-102.html)* *(in German). Archived from the original (https://www.zdf.de/dokumentation/zdfinfo-doku/darknet-hacker-cyberwar-102.html)* *on 4 April 2017. Retrieved 3 April 2017.*

Further reading

- Andress, Jason. Winterfeld, Steve. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress. ISBN 1-59749-637-5
- Bodmer, Kilger, Carpenter, & Jones (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. New York: McGraw-Hill Osborne Media. ISBN 0071772499, "ISBN 978-0071772495"
- Brenner, S. (2009). *Cyber Threats: The Emerging Fault Lines of the Nation State*. Oxford University Press. ISBN 0-19-538501-2
- Carr, Jeffrey. (2010). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly. ISBN 978-0-596-80215-8
- Conti, Gregory. Raymond, David. (2017). *On Cyber: Towards an Operational Art for Cyber Conflict*. Kopidion Press. ISBN 978-0692911563
- Cordesman, Anthony H.; Cordesman, Justin G. (2002). *Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland* (https://books.google.com/books?id=YIiRyO6ctzMC) . Greenwood Publishing Group. ISBN 978-0-275-97423-7.
- Costigan, Sean S.; Perry, Jake (2012). *Cyberspaces and global affairs*. Farnham, Surrey: Ashgate. ISBN 9781409427544.
- Fritsch, Lothar & Fischer-Hübner, Simone (2019). Implications of Privacy & Security Research for the Upcoming Battlefield of Things (http://urn.kb.se/resolve?urn=urn:nbn:se:kau:diva-71893) . Journal of Information Warfare, 17(4), 72–87.
- Gaycken, Sandro. (2012). *Cyberwar – Das Wettrüsten hat längst begonnen*. Goldmann/Randomhouse. ISBN 978-3442157105
- Geers, Kenneth. (2011). *Strategic Cyber Security*. NATO Cyber Centre. *Strategic Cyber Security* (https://web.archive.org/web/20180516135306/http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF) , ISBN 978-9949-9040-7-5, 169 pages

- Halpern, Sue, "The Drums of Cyberwar" (review of Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday, 2019, 348 pp.), *The New York Review of Books*, vol. LXVI, no. 20 (19 December 2019), pp. 14, 16, 20.
- Shane Harris (2014). *@War: The Rise of the Military-Internet Complex*. Eamon Dolan/Houghton Mifflin Harcourt. ISBN 978-0544251793.
- Hunt, Edward (2012). "US Government Computer Penetration Programs and the Implications for Cyberwar" (http://www.computer.org/csdl/mags/an/2012/03/man2012030004.html) . *IEEE Annals of the History of Computing*. **34** (3): 4–21. doi:10.1109/mahc.2011.82 (https://doi.org/10.1109%2Fmahc.2011.82) . S2CID 16367311 (https://api.semanticscholar.org/CorpusID:16367311) .
- Janczewski, Lech; Colarik, Andrew M. (2007). *Cyber Warfare and Cyber Terrorism* (https://books.google.com/books?id=6CJ-aV9Dh-QC) . Idea Group Inc (IGI). ISBN 978-1-59140-992-2.
- Rid, Thomas (2012). "Cyber War Will Not Take Place". *Journal of Strategic Studies*. **35**: 5–32. doi:10.1080/01402390.2011.608939 (https://doi.org/10.1080%2F01402390.2011.608939) . S2CID 153828543 (https://api.semanticscholar.org/CorpusID:153828543) .
- Woltag, Johann-Christoph: 'Cyber Warfare' in *Rüdiger Wolfrum (Ed.) Max Planck Encyclopedia of Public International Law (Oxford University Press 2012) (http://www.mpepil.com)* .

External links

- Media related to Cyberwarfare at Wikimedia Commons
- The Information Age at Wikibooks
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (https://ccdcoe.org/)
- Cyberwar Twitter feed from Richard Stiennon (https://twitter.com/cyberwar)
- Cyberwar News community by Reza Rafati (http://cyberwarzone.com/)

Videos

- "Sabotaging the System" (https://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/) video, "60 Minutes", 8 November 2009, CBS News, 15 minutes

Articles

- ABC: Former White House security advisor warns of cyber war (http://www.abc.net.au/worldtoday/content/2010/s3086792.htm)

- Wall Street Journal: Fighting Wars in Cyberspace (https://www.wsj.com/articles/SB10001424052748703724104575379343636553602)
- Will There Be An Electronic Pearl Harbor, PC World (http://www.pcworld.com/article/183436/will_there_be_an_electronic_pearl_harbor.html) Archived (https://web.archive.org/web/20091203173305/http://www.pcworld.com/article/183436/will_there_be_an_electronic_pearl_harbor.html) 3 December 2009 at the Wayback Machine by Ira Winkler, 1 December 2009
- Senate panel: 80 percent of cyberattacks preventable (https://www.wired.com/threatlevel/2009/11/cyber-attacks-preventable/) , Wired, 17 November 2009
- Duncan Gardham, 26 June 2009, Hackers recruited to fight 'new cold war' (https://www.telegraph.co.uk/technology/news/5637243/Hackers-recruited-to-fight-new-cold-war.html) , Telegraph UK
- Stefano Mele, Jan 2016, Cyber Strategy & Policy Brief (Volume 01 – January 2016) (https://web.archive.org/web/20170609230902/http://stefanomele.it/news/dettaglio.asp?id=451)
- Stefano Mele, Jun 2013, Cyber-Weapons: Legal and Strategic Aspects (version 2.0) (https://web.archive.org/web/20161203170642/http://stefanomele.it/publications/dettaglio.asp?id=374)
- Stefano Mele, Sep 2010, Cyberwarfare and its damaging effects on citizens (https://web.archive.org/web/20110323001651/http://www.stefanomele.it/publications/dettaglio.asp?id=185)
- Cybersecurity: Authoritative Reports and Resources, US Congressional Research Service (https://web.archive.org/web/20160303222644/http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=150761)
- Why the USA is Losing The Cyberwar Against China (https://venturebeat.com/2011/11/09/losing-the-cyberwar/) , by Joseph Steinberg, VentureBeat, 9 November 2011
- Michael Riley and Ashlee Vance, 20 July 2011, Cyber Weapons: The New Arms Race (https://www.bloomberg.com/bw/magazine/cyber-weapons-the-new-arms-race-07212011.html)
- The Digital Arms Race: NSA Preps America for Future Battle (http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html) , *Der Spiegel*, January 2015

Last edited 6 days ago by 2404:0:803B:43CA:E5E9:8159:9F9F:730E