The Journal of Strategic Studies
Vol. 35, No. 1, 5–32, February 2012

Routledge
Taylor & Francis Group

Cyber War Will Not Take Place

THOMAS RID

King's College London, UK

ABSTRACT For almost two decades, experts and defense establishments the world over have been predicting that cyber war is coming. But is it? This article argues in three steps that cyber war has never happened in the past, that cyber war does not take place in the present, and that it is unlikely that cyber war will occur in the future. It first outlines what would constitute cyber war: a potentially lethal, instrumental, and political act of force conducted through malicious code. The second part shows what cyber war is not, case-by-case. Not one single cyber offense on record constitutes an act of war on its own. The final part offers a more nuanced terminology to come to terms with cyber attacks. All politically motivated cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: sabotage, espionage, and subversion.

KEY WORDS: Cyber-Security, Cyber War, Sabotage, Subversion, Espionage, Stuxnet, Information Operations

In the mid-1930s, inspired by the lead-up to World War I, the French dramatist Jean Giraudoux wrote a famous play, *La guerre de Troie n'aura pas lieu*, the Trojan War will not take place. The English playwright Christopher Fry translated the two acts in 1955 as *Tiger at the Gates*.[1] The plot is set inside the gates of the city of Troy. Hector, a disillusioned Trojan commander, tries to avoid in vain what the seer Cassandra has predicted to be inevitable: war with the Greeks. Giraudoux was a veteran of 1914 and later worked in the French foreign office. His tragedy is an eloquent critique of Europe's leaders, diplomats, and intellectuals who were, again, about to unleash the dogs of war. The play premiered in November 1935 in the Théâtre de l'Athénée in Paris, almost exactly four years before the dramatist's fears would come true.

Judging from present pronouncements about cyber war, the world seems to be facing another 1935-moment. 'Cyberwar is Coming!' declared the RAND Corporation's John Arquilla and David Ronfeldt in

[1]Jean Giraudoux, *Tiger at the Gates (La Guerre De Troie N'aura Pas Lieu)*, translated by Christopher Fry (New York: OUP 1955).

ISSN 0140-2390 Print/ISSN 1743-937X Online/12/010005-28 © 2012 Taylor & Francis
http://dx.doi.org/10.1080/01402390.2011.608939

1993.[2] It took a while for the establishment to catch on. 'Cyberspace is a domain in which the Air Force flies and fights', announced Michael Wynne, a US Air Force Secretary, in 2006. Four years later the Pentagon leadership joined in. 'Although cyberspace is a man-made domain', wrote William Lynn, America's Deputy Secretary of Defense, in a 2010 *Foreign Affairs* article, it has become 'just as critical to military operations as land, sea, air, and space'.[3] In the same year, Richard Clarke, the White House's former cyber tsar, invoked calamities of a magnitude that make 9/11 pale in comparison and urged taking a number of measures 'simultaneously and now to avert a cyber war disaster'.[4] In February 2011, then-Central Intelligence Agency Director Leon Panetta warned the House Permanent Select Committee on Intelligence: 'The next Pearl Harbor could very well be a cyber attack.'[5] That year a highly sophisticated computer worm may have significantly damaged the Iranian nuclear enrichment program at Natanz. One much-noted investigative article in *Vanity Fair* concluded that the event foreshadowed the destructive new face of twenty-first century warfare, 'Stuxnet is the Hiroshima of cyber-war.'[6]

But is it? Are the Cassandras of cyber warfare on the right side of history? Is cyber war really coming? This article argues that cyber war will not take place. That statement does not come with a Giraudouxian twist and irony. It is meant literally – as a statement about the past, the present, and the likely future: Cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future. Instead, all past and present political cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage. That is improbable to change in the years ahead.

The argument is presented in three steps. The first part outlines what cyber war is. Any attempt to answer the question of cyber war has to start conceptually. An offensive act has to meet certain criteria in order to qualify as an act of war. Any act of war has to have the potential to be lethal; it has to be instrumental; and it has to be political. The second part outlines what cyber war is not, case-by-case. Not one single past cyber offense, neither a minor nor a major one, constitutes an act of war on its own. This finding raises an immediate question, what these

[2]John Arquilla and David Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy* 12/2 (1993), 141–65.
[3]William J. Lynn, 'Defending a New Domain', *Foreign Affairs* 89/5 (2010), 101.
[4]Richard A. Clarke, and Robert K. Knake, *Cyber War* (New York: Ecco 2010), 261.
[5]Lisa Daniel, 'Panetta: Intelligence Community Needs to Predict Uprisings', *American Forces Press Service*, 11 Feb. 2011.
[6]Michael Joseph Gross, 'A Declaration of Cyber-War', *Vanity Fair*, April 2011.

events actually are, if they are not war. The final part therefore constructively offers a more nuanced terminology to come to terms with cyber attacks. Political offenses – events between apolitical crime on the one end of the spectrum and real war on the other end – may have the aim of subverting, spying, or sabotaging. All cyber offenses of the past and current years fall into these three classes of activities. The article concludes by pointing out trends, risks, and recommendations.

What is Cyber War?

Clausewitz still offers the most concise concept of war. It has three main elements. Any aggressive or defensive action that aspires to be a stand-alone act of war, or may be interpreted as such, has to meet all three criteria. Past cyber attacks do not.

The first element is war's violent character. 'War is an act of force to compel the enemy to do our will', wrote Carl von Clausewitz on the first page of *On War*.[7] All war, pretty simply, is violent. If an act is not potentially violent, it is not an act of war. Then the term is diluted and degenerates to a mere metaphor, as in the 'war' on obesity or the 'war' on cancer. A real act of war is always potentially or actually lethal, at least for some participants on at least one side. Unless physical violence is stressed, war is a hodgepodge notion, to paraphrase Jack Gibbs.[8] In Clausewitz's thinking, violence is the pivotal point of all war. Both enemies – he usually considered two sides – would attempt to escalate violence to the extreme, unless tamed by friction, imponderables, and politics.[9]

The second element highlighted by Clausewitz is war's instrumental character. An act of war is always instrumental. To be instrumental, there has to be a means and an end. Physical violence or the threat of force is the *means*. The *end* is to force the enemy to accept the offender's will. Such a definition is 'theoretically necessary', Clausewitz

[7]Carl von Clausewitz, *Vom Kriege* (Berlin: Ullstein 1832, 1980), 27.

[8]One of the most creative and important theoreticians of deterrence, Jack Gibbs, once pointed out that fear and the threat of force are integral ingredients of deterrence, 'Unless threat and fear are stressed, deterrence is a hodgepodge notion.' Jack P. Gibbs, 'Deterrence Theory and Research', in Gary Melton, Laura Nader and Richard A. Dienstbier (eds), *Law as a Behavioral Instrument* (Lincoln: Univ. of Nebraska Press 1986), 87.

[9]Thomas Mahnken, in a useful conceptual appraisal of cyber war, also uses Clausewitz's definition of war as violent, political, and 'interactive', and argues that the basic nature of war was neither fundamentally altered by the advent of nuclear weapons nor by cyber attack. Thomas G. Mahnken, 'Cyber War and Cyber Warfare', in Kristin Lord and Travis Sharp (eds), *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. 2 (Washington DC: CNAS 2011), 53–62.

argued.[10] To achieve the end of war, one opponent has to be rendered defenseless. Or, to be more precise: the opponent has to be brought into a position, against his will, where any change of that position brought about by the continued use of arms would bring only more disadvantages for him, at least in that opponent's view. Complete defenselessness is only the most extreme of those positions. Both opponents use violence in this instrumental way, shaping each other's behavior, giving each other the law of action, in the words of the Prussian philosopher of war.[11] The instrumental use of means takes place on tactical, operational, strategic, and political levels. The higher the order of the desired goal, the more difficult it is to achieve. As Clausewitz put it, in the slightly stilted language of his time: 'The purpose is a political intention, the means is war; never can the means be understood without the purpose.'[12] This leads to another central feature of war.

The third element that Clausewitz identified is war's political nature. An act of war is always political. The objective of battle, to 'throw' the enemy and to make him defenseless, may temporarily blind commanders and even strategists to the larger purpose of war. War is never an isolated act. War is never only one decision. In the real world, war's larger purpose is always a political purpose. It transcends the use of force. This insight was captured by Clausewitz's most famous phrase, 'War is a mere continuation of politics by other means.'[13] To be political, a political entity or a representative of a political entity, whatever its constitutional form, has to have an intention, a will. That intention has to be articulated. And one side's will has to be transmitted to the adversary at some point during the confrontation (it does not have to be publicly communicated). Any violent act and its larger political intention also has to be attributed to one side at some point during the confrontation. History does not know acts of war without eventual attribution.

One modification is significant before applying these criteria to cyber offenses. A pivotal element of any warlike action remains the 'act of force'. That act of force is usually rather compact and dense, even when its components are analyzed in detail. In most armed confrontations, be they conventional or unconventional, the use of force is more or less straightforward: it may be an F-16 striking targets from the air, artillery

[10]Clausewitz, *Vom Kriege*, 29.
[11]'[Der Gegner] gibt mir das Gesetz, wie ich es ihm gebe', ibid., 30.
[12]Ibid., 35.
[13]In *Vom Kriege*, Clausewitz uses similar phrases a few times. This quote is a translation of the heading of Book 1, Chapter 24, 'Der Krieg ist einer bloße Fortsetzung der Politik mit anderen Mitteln', ibid., 44.

barrages, a drone-strike, improvised explosive devices placed by the side of a road, even a suicide bomber in a public square. In all these cases, a combatant's or insurgent's triggering action – say pushing a button or pulling trigger – will rather immediately and directly result in casualties, even if a timer or a remote control device is used, such as a drone or a cruise missile, and even if a programmed weapon system is able to semi-autonomously decide which target to engage or not.[14] An act of cyber war would be an entirely different game.

In an act of cyber war, the actual use of force is likely to be a far more complex and mediated sequence of causes and consequences that ultimately result in violence and casualties.[15] One often-invoked scenario is a Chinese cyber attack on the United States homeland in case of a political crisis in, say, the Taiwan Strait. The Chinese could blanket a major city with blackout by activating so-called logic-bombs that were pre-installed in America's electricity grid. Financial information on a massive scale could be lost. Derailments could crash trains. Air traffic systems and their backups could collapse, leaving hundreds of planes aloft without communication. Industrial control systems of highly sensitive plants, such as nuclear power stations, could be damaged, potentially leading to loss of cooling, meltdown, and contamination.[16] As a result, people could suffer serious injuries or be killed. Military units could be rendered defenseless. In such a scenario, the causal chain that links somebody pushing a button to somebody else being hurt is mediated, delayed, and permeated by chance and friction. Yet such mediated destruction caused by a cyber offense *could*, without doubt, be an act of war, even if the means were not violent, only the consequences.[17] Moreover, in highly networked societies, non-violent cyber attacks *could* cause economic consequences without violent effects that then *could* exceed the harm of an otherwise smaller physical attack.[18] For one thing, such scenarios have caused widespread confusion, 'Rarely has something been so important and so talked about with less clarity and less apparent understanding than this

[14]This statement is not statement about the different levels of war: connecting between the political, strategic, operation, and tactical levels always remains a challenge.

[15]This problem has been extensively discussed also among legal scholars. For an excellent recent overview, see Matthew C. Waxman, 'Cyber-Attacks and the Use of Force', *The Yale Journal of International Law* 36 (2011), 421–59.

[16]For a particularly vividly told scenario, see the opening scene of Clarke and Knake, *Cyber War*.

[17]See, for instance, Yoram Dinstein, 'Computer Network Attacks and Self-Defense', *International Law Studies* 76 (2002), 103. Arguing from a legal perspective, Dinstein also stresses 'violent consequences'.

[18]More on this argument, Waxman, 'Cyber-Attacks and the Use of Force', 436.

phenomenon', commented Michael Hayden, formerly director of the CIA as well as the National Security Agency (NSA).[19] And second, to date all such scenarios have another major shortfall: they remain fiction, not to say science fiction.

Not Cyber War

If the use of force in war is violent, instrumental, and political, then there is no cyber offense that meets all three criteria. But more than that, there are very few cyber attacks in history that meet only *one* of these criteria. It is useful to consider the most-quoted offenses case-by-case, and criterion-by-criterion.

The most violent 'cyber' attack to date is likely to be a Siberian pipeline explosion – if it actually happened. In 1982, an American covert operation allegedly used rigged software to cause a massive pipeline explosion in Russia's Urengoy–Surgut–Chelyabinsk pipeline, which connected the Urengoy gas fields in Siberia across Kazakhstan, then Russia, to European markets. The gigantic pipeline project required sophisticated control systems, for which the Soviet operators had to purchase computers on the open markets. The Russian pipeline authorities tried to acquire the necessary Supervisory Control and Data Acquisition software, known as SCADA, from the United States and were turned down. The Russians then attempted to get the software from a Canadian firm. The CIA is said to have succeeded in inserting malicious code into the control system that ended up being installed in Siberia. The code that controlled pumps, turbines, and valves was programmed to operate normally for a time and then 'to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds', recounted Thomas Reed, an official in the National Security Council at the time.[20] In June 1982, the rigged valves probably resulted in a 'monumental' explosion and fire that could be seen from space. The US Air Force allegedly rated the explosion at three kilotons, equivalent to a small nuclear device.[21] But when Reed's book came out in 2004, Vasily Pchelintsev, a former KGB head of the Tyumen region where the alleged explosion was supposed to have taken place, denied the story. He surmised that Reed could have referred to an explosion that happened not in June but on a warm April day that year, 50 kilometers from the city of Tobolsk, caused by

[19]Michael V. Hayden, 'The Future of Things "Cyber"', *Strategic Studies Quarterly* 5/1 (Spring 2011) 3.
[20]Thomas C. Reed, *At the Abyss* (New York: Random House 2004), 268–9.
[21]Clarke and Knake, *Cyber War*, 93.

shifting pipes in the tundra's melting ground. No one was hurt in that explosion.[22]

There are no media reports from 1982 that would confirm Reed's alleged explosion, although regular accidents and pipeline explosions in the USSR were reported in the early 1980s. Even after the CIA declassified the so-called Farewell Dossier, which described the effort to provide the Soviet Union with defective technology, the agency did not confirm that such an explosion took place. If it happened, it is unclear if the explosion resulted in casualties. The available evidence on the event is so thin and questionable that it cannot be counted as a proven case of a successful logic bomb. This means that there is no known cyber attack that unequivocally meets Clausewitz's first criterion: violence. No cyber offense has ever caused the loss of human life. No cyber offense has ever injured a person. No cyber attack has ever damaged a building.[23]

Another oft-quoted example of cyber war is an attack on Estonia that began in late April 2007. Estonia at the time was one of the world's most connected nations; two thirds of all Estonians used the Internet and 95 percent of banking transactions were done electronically.[24] The small and well-wired Baltic country was relatively vulnerable to cyber attacks. The story started about two weeks before 9 May, a highly emotional day in Russia when the victory against Nazi Germany is remembered. With indelicate timing, authorities in Tallinn decided to move the two-meter Bronze Soldier, a Russian World War II memorial of the Unknown Soldier, from the center of the capital to its outskirts. The Russian-speaking populations as well as neighboring Russia were aghast. On 26 and 27 April, Tallinn saw violent street riots, with 1,300 arrests, 100 injuries, and one fatality.

The street riots were accompanied by online riots. The cyber attacks started in the late hours of Friday 27 April. Initially the attackers used rather inept, low-technology methods, such as ping floods and simple denial of service attacks. Then the attacks became slightly more sophisticated. Starting on 30 April, simple botnets were used to

---

[22]Anatoly Medetsky, 'KGB Veteran Denies CIA Caused '82 Blast', *Moscow Times*, 18 March 2004.

[23]An accidental gasoline explosion that occured in Bellingham, WA on 10 June 1999, is sometimes named as a violent cyber incident; three youths were killed. Although the relevant SCADA system was found directly accessible by dial-in modem, no evidence of hacking was uncovered in the official government report. See, National Transportation Safety Board, 'Pipline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999', Pipeline Accident Report NTSB/PAR-02/02 (Washington DC, 2002), 64.

[24]Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents* (Tallinn: CCDCOE 2010), 17.

increase the volume of distributed denial of service (DDoS) attacks, and the timing of these collective attacks was increasingly coordinated. Other types of nuisances included email and comment spam as well as the defacement of the Estonian Reform Party's website. Estonia experienced what was then the worst-ever DDoS. The attacks came from an extremely large number of hijacked computers, up to 85,000; and the attacks went on for an unusually long time, for three weeks, until 19 May. The attacks reached a peak on 9 May, when Moscow celebrates Victory Day. Fifty-eight Estonian websites were down at once. The online services of Estonia's largest bank, then known as Hansapank, were unavailable for 90 minutes on 9 May and for two hours a day later.[25] The effect of these coordinated online protests on business, government, and society was noticeable, but ultimately it remained minor. The main long-term consequence of the attack was that the Estonian government succeeded in getting the North Atlantic Treaty Organization (NATO) to establish a permanent agency in Tallinn, the Cooperative Cyber Defence Centre of Excellence.

A few things are notable about the attack. It remained unclear who was behind the attacks. Estonia's defense minister as well as the country's top diplomat pointed their fingers at the Kremlin. But they were unable to muster evidence, retracting earlier statements that Estonia had been able to trace the Internet Provider addresses of some computers involved in the attack back to the Russian government. Neither experts from the Atlantic Alliance nor from the European Commission were able to identify Russian fingerprints in the operations. Russian officials called accusations of involvement 'unfounded'.[26]

Keeping Estonia's attack in perspective is important. Mihkel Tammet, an official in charge of Information Computer Technology (ICT) for the Estonian Ministry of Defense, described the time leading up to the launch of the attacks as a 'gathering of botnets like a gathering of armies'.[27] Andrus Ansip, then Estonia's prime minister, asked, 'What's the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and

[25]These disruptions were the worst of the entire 'cyber war' according to ibid., 20.

[26]'Estonia has no evidence of Kremlin involvement in cyber attacks', *Ria Novosti*, 6 Sept. 2007. It should also be noted that Russian activists and even a State Duma Deputy (although perhaps jokingly) have claimed to be behind the attacks, see Gadi Evron, 'Authoritatively, Who was Behind the Estonian Attacks?' *Darkreading*, 17 March 2009. See also, Gadi Evron, 'Battling Botnets and Online Mobs', *Science & Technology* (Winter/Spring 2008), 121–8.

[27]Tim Espiner, 'Estonia's cyberattacks: lessons learned, a year on', *ZDNet UK*, 1 May 2008.

newspaper websites?'[28] It was of course a rhetorical question. Yet the answer is simple: unlike a naval blockade, the mere 'blockade' of websites is not violent, not even potentially; unlike a naval blockade, the DDoS attack was not instrumentally tied to a tactical objective, but an act of undirected protest; and unlike ships blocking the way, the pings remained anonymous, without political backing. Ansip could have asked what the difference was between a large popular demonstration blocking access to buildings and the blocking of websites. The comparison would have been better, but still flawed for an additional reason: many more actual people have to show up for a good old-fashioned demonstration than for a DDoS attack.

A year later a third major event occurred that would enter the Cassandra's tale of cyber war. The context was a ground war between the Russian Federation and Georgia in August 2008. The short armed confrontation was triggered by a territorial dispute over South Ossetia. On 7 August, the Georgian Army reacted to provocations by attacking South Ossetia's separatist forces. One day later, Russia responded militarily. Yet the computer attack on the Georgian websites started slowly on 29 July, ten days before the military confrontation and with it the main cyber attack started on 8 August. It may have been the first time an independent cyber attack happened in synchronization with a conventional military operation. The cyber attacks on Georgia comprised three types.

Some of the country's prominent websites were defaced, for instance that of Georgia's national bank and the ministry of foreign affairs. The most notorious defacement was a collage of portraits juxtaposing Adolf Hitler and Mikheil Saakashvili, the Georgian president.

The second type of offence were denial-of-service attacks against websites in the Georgian public and private sectors, including government websites, like the parliament, but also news media, Georgia's largest commercial bank, and other minor websites. The attacks, on average, lasted around two hours and 15 minutes, the longest up to six hours.[29]

A third method was an effort to distribute malicious software to deepen the ranks of the attackers and the volume of attacks. Various Russian-language forums helped distribute scripts that enabled the public to take action, even posting the attack script in an archived

[28]Андрей Злобин, Ксения Болецкая, 'Электронная бомба,' *Ведомости* [Andrey Zlobin and Xenia Boletskaya, 'E-bomb', *Vedomosti*] 28 May 2007, <http://bitly.com/g1M9Si>.

[29]The intensity of the attacks was high, with traffic reaching 211.66 Mbps on average, peaking at 814.33 Mbps, see Jose Nazario, 'Georgia DDoS Attacks – A Quick Summary of Observations', *Security to the Core (Arbor Networks)*, 12 Aug. 2008.

version, *war.rar*, which prioritized Georgian government websites. In a similar vein, email addresses of Georgian politicians were spammed.

The effects of the attack were again rather small. Despite the warlike rhetoric by the international press, by the Georgian government, and by anonymous hackers, the attacks were not violent. And Georgia, a small country with a population of about 4.5 million, was even less vulnerable to attacks than Estonia; web access was relatively low and few vital services like energy, transportation, or banking were tied to the Internet. The attack had little effect beyond making a number of Georgian government websites temporarily inaccessible. The attack was also only minimally instrumental. The attack's main damage was in limiting the government's ability to communicate internationally and making the small country's voice heard at a critical moment. If the attackers intended this effect, its utility was limited: the foreign ministry took the rare step, with Google's permission, to set up a weblog on Blogger, the company's blogging platform. This helped keep one more channel to journalists open. The National Bank of Georgia ordered all branches to stop offering electronic services for ten days. Most importantly, the attack was not genuinely political in nature. As in the Estonian case, the Georgian government blamed the Kremlin. But Russia again denied official sponsorship of the attacks. NATO's Tallinn-based cyber security center published a report on the Georgia attacks. Although the attacks appeared coordinated and instructed, and although the media were pointing fingers at Russia, 'there is no conclusive proof of who is behind the DDoS attacks', NATO concluded, 'as was the case with Estonia'.[30]

The cyber scuffles that accompanied the street protests in Estonia and the short military ground campaign in Georgia were precedents. Perhaps the novelty of these types of offenses was the main reason for their high public profile and the warlike rhetoric that surrounded them. The same observation might be true for another type of 'cyber war', high-profile spying operations. An early example is 'Moonlight Maze'. That lurid name was given to a highly classified cyber-espionage incident discovered in 1999. The US Air Force coincidentally discovered the intrusion into its network. The Federal Bureau of Investigation (FBI) was alerted. The federal investigators called in the NSA. An investigation uncovered a pattern of intrusion into computers

[30]Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm and Liis Vihul, *Cyber Attacks against Georgia* (Tallinn: CCDCOE 2008), 12. Jeffrey Carr, a cyber security expert, published a report that concluded that Russia's Foreign Military Intelligence Agency (GRU) and Federal Security Service (FSB) probably helped coordinate the attacks, not independent patriotic hackers. But to date, this was neither proven nor admitted.

at the National Aeronautics and Space Administration (NASA), at the Energy Department, at universities as well as research laboratories that had started in March 1998. Maps of military installations were copied, hardware designs, and other sensitive information. The incursions went on for almost two years. The Pentagon was able to trace back the attack to what was then called a mainframe computer in Russia. But again: no violence, unclear goals, no political attribution.

Yet the empirical trend is obvious: over the past dozen years, cyber attacks have been steadily on the rise. The frequency of major security breaches against governmental and corporate targets has been going up. The volume of attacks is increasing. So is the participation in attacks, ranging from criminals to activists to the NSA. The range of aggressive behavior online is widening. At the same time the sophistication of some attacks has reached new heights. In this respect Stuxnet has indeed been a game-changing event. Despite these trends the 'war' in 'cyber war' has more in common with the 'war' on obesity than with the World War II – it has more metaphoric than descriptive value. It is high time to go back to classic terminology and understand cyber offences for what they really are.

Aggression, whether it involves computers or not, may be criminal or political in nature. It is useful to group offences along a spectrum, stretching from ordinary crime all the way to conventional war. Then a few distinctive features become visible: crime is mostly apolitical, war is always political; criminals conceal their identity, uniformed soldiers display their identity openly. Political violence (or 'political crime' in criminology and the theory of law) occupies the muddled middle of this spectrum, being neither ordinary crime nor ordinary war. For reasons of simplicity, this analysis will focus on three types of offenses on that middle stretch of the spectrum: subversion, espionage, and sabotage. All three activities may involve states as well as private actors. Cyber offenses tend to be skewed towards the criminal end of the spectrum. So far there is no known act of cyber war, when war is properly defined. That of course does not mean that there are no political cyber offenses. But all known political cyber offenses, criminal or not, are neither common crime nor common war. Their purpose is subverting, spying, or sabotaging.

In all three cases, Clausewitz's three criteria are jumbled. These activities need not be violent to be effective. They need not be instrumental to work, as subversion may often be an expression of collective passion and espionage may be an outcome of opportunity rather than strategy. And finally: aggressors engaging in subversion, espionage or sabotage do act politically; but in sharp contrast to warfare, they are likely to have a permanent or at least temporary interest in avoiding attribution. This is one of the main reasons why

political crime, more than acts of war, has thrived in the cyber domain, where non-attribution may be easier to achieve than waterproof attribution. It goes without saying that subversion, espionage and sabotage – 'cybered' or not – may accompany military operations. Both sides may use it, and indeed have done so since time immemorial. But the advent of digital networks had an uneven effect.

Sabotage

Sabotage, first, is a deliberate attempt to weaken or destroy an economic or military system. All sabotage is predominantly *technical* in nature, but of course may use social enablers. The word allegedly dates from a French railway strike in 1910. Workers removed and damaged the *sabots*, wooden shoes that held the rails in their bed. The means used in sabotage must not always lead to physical destruction and overt violence, but they can. *If violence is used, things are the prime targets, not humans*, even if the ultimate objective may be to change the cost-benefit calculus of decisionmakers. Sabotage tends to be tactical in nature and will only rarely have operational or even strategic effects. The higher the technical development and the dependency of a society and its government and military, the higher is the potential for sabotage, especially cyber-enabled sabotage. Sabotage on its own may not be an act of war because the saboteurs may deliberately avoid open violence, they may avoid political attribution, but they always aim to be instrumental. Both avoiding excessive violence and avoiding identification may serve the ultimate goal of sabotage: impairing a technical system. Two high-profile sabotage operations, both Israeli, are instructive.

Some examples of successful use of cyber sabotage are publicly known. Such sabotage may happen in conjunction with conventional military force or stand-alone. One of the most spectacular examples for a combined strike is Operation 'Orchard', Israel's bombing raid on a nuclear reactor site at Dayr ez-Zor in northern Syria on 6 September 2007. It appears that the Israeli Air Force prepared for the main attack by taking out a single Syrian radar site at Tall al-Abuad close to the Turkish border. The Israeli attackers combined electronic warfare with precision strikes. The Syrian electrical grid was not affected. Syria's air-defense system, one of the most capable in the world, went blind and failed to detect an entire Israeli squadron of F-15I and F-16I warplanes entering Syrian airspace, raiding the site, and leaving again.[31] Before-and-after satellite pictures of the targeted site on the Euphrates were

[31]David A. Fulghum, Robert Wall and Amy Butler, 'Israel Shows Electronic Prowess', *Aviation Week & Space Technology* 168, 25 Nov. 2007; David A. Fulghum, Robert

made public by the US government. They show that the nascent nuclear facility with its suspected reactor building, which was located about 145 kilometers from Iraq, had been reduced to rubble. The cyber work of the operation was probably done by Unit 8200, the largest unit in the Israel Defense Forces (IDF) and Israel's equivalent to the NSA.[32] The technicians may have used a so-called 'kill switch' embedded in the air defense system by a contractor to render it useless.[33] The details of the operation remain highly classified. But one thing can be highlighted already: the cyber element of Operation 'Orchard' probably was critical for the success of the Israeli raid and although the cyber attack did not physically destroy anything on its own right, it should be seen as an integrated part of a larger military operation. Although the cyber attack on its own – without the military component – would not have constituted an act of war, it was nevertheless an enabler for a successful military attack. That was different in another, even more spectacular recent incident.

Stuxnet was by far the most sophisticated known cyber attack to date. It was a highly directed attack against specific targets, most likely Iran's nuclear enrichment program at Natanz.[34] The worm was an act of cyber-enabled stand-alone sabotage not connected to a conventional military operation. Stuxnet was what the security industry calls an Advanced Persistent Threat (APT). Operation 'Myrtus,' as Stuxnet may have been called by its creators, was a multi-year campaign. The program started probably in late 2007 or early 2008.[35] It is likely that the main attack had been executed between June 2009 and June 2010, when Information Technology (IT) security companies first publicly mentioned the worm. Stuxnet recorded a timestamp and other system information. Therefore engineers were able, in months of hard work, to outline the worm's infection history as well as to reverse-engineer the threat and to understand its purpose. The following paragraphs are intended to provide a glimpse into Stuxnet's complexity and sophistication.

The sabotage software was specifically written for Industrial Control Systems. These control systems are box-shaped stacks of hardware without keyboards or screens. A so-called Programmable Logic

---

Wall and Amy Butler, 'Cyber-Combat's First Shot', *Aviation Week & Space Technology* 167, 16 Nov. 2007, 28–31.

[32]John Markoff, 'A silent attack, but not a subtle one', *New York Times*, 26 Sept. 2010.

[33]Sally Adee, 'The Hunt for the Kill Switch', *IEEE Spectrum*, May 2008.

[34]Gross, 'A Declaration of Cyber-War'.

[35]Ralph Langner, 'What Stuxnet is All About', *The Last Line of Cyber Defense*, 10 Jan. 2011.

Controller (PLC) runs the control system. Therefore an industrial plant's operators have to program the controllers by temporarily hooking them up to a laptop, most likely a so-called Field PG, a special industrial notebook sold by Siemens. These Field PGs, unlike the control system and the controller itself, run Microsoft Windows and were most likely not connected to the Internet and not even to an internal network.[36]

The first complication for the attackers was therefore a feasible infection strategy. Stuxnet had to be introduced into the target environment and spread there in order to reach its precise target. That target was protected by a so-called 'air gap', by not being connected to the insecure Internet and even internal networks. Therefore the infection most likely happened through a removable drive, such as a USB stick. The attack vehicle was coded in a way that allowed its handlers to connect to the worm through a command-and-control server. But because the final target was not networked, 'all the functionality required to sabotage a system was embedded directly in the Stuxnet executable', Symantec observed in the updated *W32.Stuxnet Dossier*, an authoritative analysis of the worm's code.[37] The worm's injection mechanism had to be aggressive. The number of collateral and inconsequential infections was initially large: by the end of 2010, the worm had infected approximately 100,000 hosts in dozens of countries, 60 percent of which were in Iran – the machines that ultimately spread the virus on its two final targets were among them.

A second complexity was Stuxnet's 'sabotage strategy', in Symantec's words. The work specifically targeted two models of Siemens logic controllers, 6ES7-315-2 and 6ES7-417, so-called code 315 and code 417. The likely targets were the K-1000–60/3000–3 steam turbine in the Bushehr nuclear power plant for code 417 and the gas centrifuges in Natanz for code 315.[38] If the worm was able to connect to such controllers, it proceeded checking their configurations to identify the target. If Stuxnet did not find the right configuration, it did nothing. But if it found what it was looking for, the worm started a sequence to inject one of three payloads. These payloads were coded to change the output frequencies of specific drivers that run motors. Stuxnet thus was set up to cause industrial processes to malfunction, physically damaging

[36]Nicolas Falliere, Liam O Murchu and Eric Chien, *W32.Stuxnet Dossier. Version 1.4* (Symantec 2011), 3.
[37]Ibid., 3.
[38]This is Ralph Langner's target theory. The question if Stuxnet's code 417 'warhead' was disabled or not is controversial among engineers. See ibid., 45 as well as Ralph Langner, 'Matching Langner's Stuxnet Analysis and Symantec's Dossier Update', *The Last Line of Cyber Defense*, 21 Feb. 2011.

rotors, turbines, and centrifuges. The attack's goal was damaging the centrifuges slowly, thus tricking the plant's operators. Their rationale probably was that damaging hardware would delay Iran's enrichment program for a significant period of time, as components cannot just be easily bought on open markets.

This method relates to a third complexity, the worm's stealthiness. Before Stuxnet started sabotaging processes, it intercepted input values from sensors, for instance the state of a valve or operating temperatures, recorded these data, and then provided the legitimate controller code with pre-recorded fake input signals, while the actual processes in the hidden background were manipulated. The objective was not just fooling operators in a control room, but circumventing and compromising digital safety systems. Stuxnet also hid the modifications it made to the controller code. And even before launching a payload, Stuxnet operated stealthily: it had mechanisms to evade antivirus software, it is able to hide copies of its files on removable drives, hide its own program blocks when an enumeration is enforced on a controller, and erased itself from machines that do not lead to the target.

The resources and investment that went into Stuxnet could only be mustered by a 'cyber superpower', argued Ralph Langner, a German control system security consultant who first extracted and decompiled the attack code.[39] A possibility is that Israel engineered the threat with American support. It starts with intelligence: each single control system is a unique configuration, so the attackers needed superb information about the specific system's schematics. 'They probably even knew the shoe size of the operators', joked Langner. The designs could have been stolen or even extracted by an earlier version of Stuxnet. Another aspect is the threat's design itself: the code was so specific that it is likely that the attackers had to set up a mirrored environment to refine their attack vehicle, which could have included a mock enrichment facility.[40] Stuxnet also had network infection routines, it was equipped with peer-to-peer update mechanisms that seem to have been capable communicating even with infected equipment without Internet connection, and injected code into industrial control systems while hiding the code from the operator. Programming such a complex agent required time, resources, and an entire team of core developers as well as quality assurance and management.[41] The threat also combined expensive and hard-to-get items: four zero-day exploits, two stolen

[39]Ralph Langner, 'Cracking Stuxnet', *TED Talk*, March 2011.

[40]William J. Broad, John Markoff and David E. Sanger, 'Israeli test on worm called crucial in Iran nuclear delay', *New York Times*, 16 Jan. 2011, A1.

[41]Nicolas Falliere, Liam O Murchu and Eric Chien, *W32.Stuxnet Dossier. Version 1.4* (Symantec 2011), 3.

digital certificates, a Windows rootkit (a software granting hidden privileged access), and even the first-ever Programmable Logic Controller rootkit.[42] For the time being it remains unclear how successful the Stuxnet attack against Iran's nuclear program actually was. But it is clear that the operation has taken computer sabotage to an entirely new level.

Espionage

The second offensive activity that is neither crime nor war is espionage. Espionage is an attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information. It may be either *social* or *technical* in nature. That division of labour is old. It is known as human intelligence and signals intelligence in the trade of secret services. The level of technical sophistication required for espionage may be high, but the requirements are less demanding than for complex sabotage operations. This is because espionage is not directly instrumental; its main purpose is not achieving a goal but to gather the information that may be used to design more concrete instruments or policies. A highly digitized environment has vastly increased the number of actors in the espionage business. Professionally and expensively trained agents working for governments (or large companies) have new competition from hackers and private individuals, sometimes acting on their own initiative yet potentially providing information for a larger cause. The most widespread use of state-sponsored cyber capabilities is for purposes of espionage. Empirically, the vast majority of all political cyber security incidents have been cases of espionage. As the attackers' identity often remains dubious, it is the victim that chooses the colorful names of these operations.

An early example, 'Moonlight Maze', has already been mentioned. Another example, 'Titan Rain', is the US government codename for a series of attacks on military and governmental computer systems in 2003, an attack that continued persistently for years. Chinese hackers had probably gained access to hundreds of firewalled networks at the Pentagon, the State Department, Homeland Security, as well as defense contractors such as Lockheed Martin. It remains unclear if Chinese security agencies were behind the intrusion or if an intruder merely wanted to mask his true identity by using China-based computers. One Pentagon source estimated that Chinese intruders had downloaded '10

[42]See Gary McGraw's discussion with Ralph Langner on Cigital's *Silver Bullet*, 25 Feb. 2011, <www.cigital.com/silverbullet/show-059/>.

to 20 terabytes of data' from non-classified Department of Defense networks.[43] Classified networks were probably not compromised.[44]

In November 2008, the US military witnessed the most significant breach of its computers to date. An allegedly Russian piece of spyware was inserted through a flash drive into a laptop at a base in the Middle East, 'placed there by a foreign intelligence agency', according to the Pentagon's number two.[45] It then started scanning the Internet for dot-mil domain addresses. This way the malware got access to the Pentagon's unclassified network, the Non-classified Internet Protocol Router Network (NIPRNET). The Defense Department's global secure intranet, the Secret Internet Protocol Router Network (SIPRNET), designed to transmit confidential and secret-level information, is protected by a so-called air gap or air wall, meaning that the secure network is physically, electrically, and electromagnetically separated from insecure networks. So once the piece of malware was on a hard drive in the NIPRNET, it began copying itself onto removable thumb drives. The hope was that an unknowing user would carry it over the air gap into SIPRNET, a problem known as the 'sneakernet' effect among the Pentagon's security experts.[46] That indeed happened and a virtual beachhead was established. But it remains unclear if the software was able to extricate information from the classified network, let alone what and how much.

In March 2009, Ron Deibert and his team at the University of Toronto publicized their discovery of what they called GhostNet, a sophisticated international spying operation, probably of Chinese origin. The network had infected 1,295 host computers of ministries of foreign affairs, embassies, international organizations, news media, and non-governmental organizations in 103 countries. The malware was able to take full control of infected computers, including searching and downloading documents, logging keystrokes, and even covertly activating personal computer cameras and microphones and capturing the recorded information.[47]

Only rarely do governments disclose information on successful cyber attacks on their systems. If they do, as some high-profile cases in the

[43]Ellen Nakashima and Brian Krebs, 'Contractor blamed in DHS data breaches', *Washington Post*, 24 Sept. 2007, A1.
[44]Bradley Graham, 'Hackers attack via Chinese web sites', *Washington Post*, 25 Aug. 2005.
[45]William J. Lynn, 'Defending a New Domain', *Foreign Affairs* 89/5 (2010), 97. Clarke says the spyware was of Russian origin, see next footnote.
[46]Clarke and Knake, *Cyber War*, 171.
[47]Ron Deibert, and Rafal Rohozinsky, *Tracking Ghostnet* (Toronto: Munk Centre for International Studies 2009), 47.

Pentagon illustrate, the amount of information released is not very deep. And not always are IT security firms or independent researchers able to analyze and illuminate the threat, like in the case of Stuxnet or Ghostnet. Therefore numerous examples exist where public information is scarce. In December 2007, the head of British internal intelligence, MI5, informed the executives of 300 companies that they were under attack by Chinese organizations, top banks among them.[48] Between 2007 and 2009, terabytes of data on the development of the F-35 were stolen, including specifics of its electronic warfare systems, the greatest advance of America's new fourth-generation fighter.[49] In January 2011, the British Foreign Office's IT system had come under attack from a 'hostile state intelligence agency'.[50] Many more past and recent examples could be added to this list, and it will certainly grow in the future. Despite heavy investments in defenses, cyber espionage is a booming activity, both against private and public entities.

Subversion

The remaining third offensive activity is subversion. Subversion is the deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order. The ultimate goal of subversion may be overthrowing a society's established government. But subversive activity may also have more limited causes, such as undermining an organization's or even a person's authority. The modus operandi of subversive activity is eroding *social* bonds, beliefs, and trust in the state and other collective entities. The means used in subversion may not always include overt violence. One common tool of subversion is propaganda, for instance pamphlets, literature, and film. The vehicle of subversion is always influencing the loyalties of individuals and uncommitted bystanders. *Human minds are the targets, not machines.* This also applies when force comes into play. It is important to note that subversion is a broader concept than insurgency: subversion, in contrast to insurgency, does not require violence and it does not require the overthrow of an established order to be successful.

To understand subversion's potentially limited instrumentality, something rather un-technical has to be considered: emotional causes. The present uses of the concept of 'cyber war' tend to be inept and

[48]Rhys Blakely, 'MI5 alert on China's cyberspace spy threat', *The Times*, 1 Dec. 2007, 1.
[49]Clarke and Knake, *Cyber War*, 232–4.
[50]Charles Arthur, 'William Hague reveals hacker attack on Foreign Office in call for cyber rules', *Guardian*, 6 Feb. 2011.

imprecise. But other classic concepts of the study of war retain their relevance and pertinence for the study of cyber offenses. Clausewitz, and many other strategic thinkers, consistently highlighted the role of passions and emotions in conflict, be it regular or irregular conflict. 'The intensity of action', Clausewitz observed, 'is a function of the motive's strength that is driving the action.' That motive may be a rational calculation or it may be emotional indignation (*Gemütserregung*), he added. 'If power is meant to be great, the latter can hardly be missing.'[51] Subversion, like insurgency, is driven by strong motives that mobilize supporters, volunteers, and activists – and, if violence comes into play, fighters and insurgents.

Another revered military thinker, David Galula, described the driving force behind an insurgent group as the cause. An insurgency's treasure would be a 'monopoly of a dynamic cause', wrote the French counterinsurgency expert in the 1960s.[52] But 50 years later, the demise of grand ideologies[53] and the rise of highly networked movements have altered the logic of dynamic causes. Not grand narratives, but highly specific issues are likely to mobilize a critical mass of enraged activists, if only temporarily. Non-attribution has lowered the costs and risks of activism – but it has also lowered the costs and risks of stopping activism again. Consequently the potential for subversion is changing: entering into subversive activity has become easier, but taking subversion a critical step further into the realm of actual politics, to successful insurgency and ultimately to governance, has become harder.[54] Three brief examples will illustrate this point.[55]

A highly insightful example for non-violent subversion is Anonymous, a loose and leaderless movement of activists. Supporters conceal their identities and unite around a self-defined cause, often promoting free speech and agitating against censorship. The movement's motto is frequently posted at the end of announcements: *We are*

[51]'Die *Energie* des Handels drückt die Stärke des Motivs aus, wodurch das Handel hervorgerufen wird, das Motiv mag nun in einer Verstandesüberzeugung oder einer Gemütserregung seinen Grund haben. Die letztere darf aber schwerlich fehlen, wo sich eine große Kraft zeigen soll.' Clausewitz, *Vom Kriege*, 69.

[52]David Galula, *Counterinsurgency Warfare: Theory and Practice* (New York: Praeger 1964), 71.

[53]For a historical discussion of ideology's role in guerrilla war, see Walter Laqueur, *Guerrilla. A Historical and Critical Study* (Boston: Little, Brown 1976).

[54]Thomas Rid and Marc Hecker, 'The Terror Fringe', *Policy Review* 158 (Dec./Jan. 2010), 3–19.

[55]For a more exhaustive list of politically motivated cyber-attacks, see Robin Gandhi, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu and Phillip Laplante, 'Dimensions of Cyber Attacks', *IEEE Technology and Society Magazine* (Spring 2011), 28–38.

Anonymous. We are Legion. We do not forgive. We do not forget. Expect us. The actions undertaken by Anonymous activists may have a political agenda or they may just be a crude form of entertainment.[56] Volunteers may be 'doing it for the lulz', as a phrase from internet culture has it. 'Lulz' is a concept related to the German idea of *Schadenfreude*, derived from a plural of 'lol', which stands for laugh-out-loud.[57] An example of the latter was Anonymous' 'YouTube porn day', a concerted prankster raid on 20 May 2009 where hundreds of pornographic videos were defiantly uploaded to the popular video-sharing site, allegedly to retaliate against the removal of music videos.[58]

The movement is best known for two high-profile political operations, although it has undertaken many more. Its first big campaign, known as 'Project Chanology', targeted the Church of Scientology and was launched on 21 January 2008 with a YouTube video that has since been viewed more than four million times.[59] When Scientology tried to censor the video, Anonymous activists reacted with DDoS attacks on Scientology's website as well as several waves of demonstrations in front of the sect's main centers worldwide, often wearing Guy Fawkes masks, adopted from the film *V for Vendetta*. The global turnout on some days was as high as 8,000 protesters. The campaign was widely covered in the international press.

A second example is Anonymous' perhaps most striking operation, a devastating assault on HBGary Federal, a technology security company. HBGary's clients included the US government and companies like McAfee. The firm with the tag-line *detecting tomorrow's malware today* had analyzed GhostNet and Aurora, two of the most sophisticated known threats. In early February 2011, Aaron Barr, then its chief executive officer (CEO), wanted more public visibility and announced that his company had infiltrated Anonymous and planned to disclose details soon. In reaction, Anonymous hackers infiltrated HBGary's servers, erased data, defaced its website with a letter ridiculing the firm with a download link to a leak of more than 40,000 of its emails to The Pirate Bay, took down the company's phone

[56]A good analysis of Anonymous is Adrian Crenshaw, 'Crude, Inconsistent Threat: Understanding Anonymous', *Irongeek.com*, 28 March 2011, <http://bitly.com/e87PeA>.

[57]An explanation and a good introduction into the sense of humor of that subculture is at <http://ohinternet.com/Lulz>.

[58]In a video titled *Jonas Brother Live On Stage*, a viewer commented: 'I'm 12 years old and what is this?' The phrase, quoted in a BBC story, went on to become an Internet meme. Siobhan Courtney, 'Pornographic videos flood YouTube', *BBC News*, 21 May 2009.

[59]<www.youtube.com/watch?v=JCbKv9yiLiQ>.

system, usurped the CEO's twitter stream, posted his social security number, and clogged up fax machines.[60] Anonymous activists had used a number of methods, including SQL injection, a code injection technique that exploits faulty database requests. 'You brought this upon yourself. You've tried to bite the Anonymous hand, and now the Anonymous hand is bitch-slapping you in the face', said the letter posted on the firm's website.[61] The attack badly pummeled the security company's reputation.

The 'Anon' movement and several assorted splinter-groups, such as LulzSec or AntiSec, have subsequently gained notoriety and attracted significant media attention. The best-known attacks successfully targeted the FBI, the CIA, the Navy as well as American government contractors such as Booz Allen Hamilton, IRC Federal, ManTech, and even the British tabloid *The Sun*. As a result, several mostly young hackers were arrested worldwide. The sophistication of their attacks, it should be noted, remains limited as the attackers were mainly going after 'low hanging fruit'.[62] The specific causes that motivated the activists were as varied and fickle as the attacks themselves.

Other examples of subversion were the politically motivated DDoS attacks in Estonia and Georgia. On the one hand the target of these attacks had a social dimension: cutting the information flow between governments, the media, and its citizens, thus undermining citizens' trust in their leaders' authority and competence. On the other hand the way these attacks were executed had a stronger social dimension: many of the predominantly Russian patriotic hackers, 'hacktivists', or 'script kiddies' who voluntarily downloaded a relatively primitive attack code did so for emotional reasons, because they were outraged by what they saw as anti-Russian policies, perhaps because they wanted to impress peers. Pulling off such an attack is relatively simple, requiring 'just a lot of people getting together and running the same tools on their home computers,' wrote Jose Nazario of Arbor Networks about the Estonia incident.[63] Steven Adair of *Shadow Server* concluded, 'The average user

[60]Peter Bright, 'Anonymous speaks: the inside story of the HBGary hack', *Ars Technica*, 15 Feb. 2011.

[61]Anonymous, 'This Domain Has Been Seized …', archived at <http://bitly.com/hWvZXs>.

[62]See 'AnonyLulzyAntiSec, Just What Have You Done for Us Lately?,' *Krypt3ia*, 22 July 2011, <http://bitly.com/qQJwiu>

[63]Charles Clover, 'Kremlin-backed group behind Estonia cyber blitz', *Financial Times*, 11 March 2009. See also Jose Nazario, 'Politically Motivated Denial of Service Attacks', in Christian Czosseck and Kenneth Geers (eds), *The Virtual Battlefield*, (Amsterdam; Washington, DC: IOS Press 2009), 163–81.

is now getting involved and helping to attack Georgian websites.' He dubbed this the 'grass roots effect' of cyber attacks.[64]

Another such example is the tussle between Israeli and Arab activists that played out during Operation 'Cast Lead' in January 2009. Many Israeli websites, often from small companies, were defaced during the short war. One simple pro-Palestinian attack tool was named after Mohammad al-Durra, a Palestinian child allegedly killed by Israeli soldiers in 2000. One notable pro-Israeli initiative was a voluntary botnet, 'Help Israel Win', which allowed individuals to voluntarily delegate control of their computers to the botnet server after downloading the 'Patriot DDoS tool', which ran in a personal computer's background while autonomously updating the client with addresses to target. The Israeli voluntary botnet was organized, according to the website's description, by 'a group of students who are tired of sitting around doing nothing while the citizens of Sderot and the cities around the Gaza Strip are suffering.'[65] In Estonia, Georgia, and Israel, riots and demonstrations were practically extended into cyberspace, even if the volunteers did not always act without the assistance of more skilled individuals.[66] In such situations, participation and (relatively) easy handling of the technology that enables participation maybe be even more significant than the sophistication of these technologies. The global jihad took this dynamic a step further.

The Internet, social media and the spread of mobile phones with video cameras had a profound effect on subversion, including subversive violence, insurgency, and even terrorism. Political violence in the twenty-first century, especially the global jihadi movement, has become an Internet-enhanced phenomenon. For jihadis, cyberspace is neither just target nor weapon, but an essential platform. That platform is used to reach out to external audiences both hostile and friendly. But more importantly it is a vehicle for internal debate and cohesion. On extremist forums, social dynamics and ideological debates among acolytes take center stage, not achieving technical prowess. Know-how of bomb-making techniques, complete with details and educational videos, are also available online. But virtual training camps cannot replace brick-and-mortar training camps, and when such substitutes were tried, the technological sophistication of attacks has dropped. Online instructional material is less important for the terrorist

[64]Steven Adair, 'Georgian Attacks: Remember Estonia?', *Shadow Server*, 13 Aug. 2008.

[65]See also Jeffrey Carr, 'Project Grey Goose Phase II Report', *GreyLogic*, 20 March 2009, Chapter 2.

[66]Rain Ottis, 'From Pitchforks to Laptops: Volunteers in Cyber Conflicts', Conference on Cyber Conflict Proceedings (2010).

movement's continuity than the ideological discussion of the various causes of resistance under the banner of jihad. Jihadism's web presence, in short, keeps alive a *strong cause at the fringe* with a persistent and stable following, albeit a small one.

An instructive counter-example is the Arab Spring of 2011. Initially the Arab youth movements that threatened the established order in Tunisia, Egypt, Libya, Syria, Yemen and elsewhere also had a web presence on social media platforms – but combined with a *strong cause in the mainstream of their societies* with a fast-growing following. Once the initial spark started a larger political movement, street protests gained a revolutionary dynamic that could barely be stopped, neither by shutting down the web nor by the state's security forces.

Conclusion

The levels of technical and social sophistication required for sabotage and subversion are inversely related. At closer inspection the required technical prowess increases from subversion, to espionage, to sabotage. The inverse applies to the required social mobilization: the mobilization of popular support is essential for subversion, perhaps helpful in espionage, and largely irrelevant for sabotage. Successful sabotage is primarily a function of the *quality* of the attacker's technical sophistication and the available intelligence; successful subversion is primarily a function of the *quantity* of supporters mobilized by the strength of political ideas and social causes. This analysis leads to three conclusions that stand in contradiction to the prophecies of cyber war.

The first conclusion is about subversion. In the past and present, not high-tech but low-tech has been more likely to lead to an escalation of violence, instability, and ultimately even war. In the twenty-first century, the one type of political offence with the greatest potential to unleash instability and violence may not be technologically highly sophisticated sabotage, but technically rather primitive subversion. Yet the Internet facilitates an unexpected effect: specific social and political causes may persist in subcultures and niche groups, either temporarily or over an extended time, either violently or non-violently – and they may never cease attracting followers yet never go mainstream. These movements may be cause-driven to a significant extent, and less dependent on leaders, organization, and mass support than classical insurgent groups. Weak causes become stronger in the sense that they garner enough support to persist over an extended period of time, constantly maintaining a self-sufficient, self-recruiting, but also self-limiting number of supporters and activists.

The second finding concerns more sophisticated cyber offenses. Conventional wisdom holds that cyberspace turns the offense/defense

balance on its head by making attacking easier and more cost-effective while making defending harder and more resource-intense. Cyber attack, the standard argument goes, increased the attacker's opportunities and the amount of damage to be done while decreasing the risks (sending special code is easier than sending special forces).[67] Hence expect more sabotage and more saboteurs. This may have it exactly wrong: quality matters more than quantity. The number of actors that are able to pull off an offensive and complex Stuxnet-class sabotage operation is likely to be smaller than commonly assumed. Cyber sabotage can be more demanding than the brick-and-mortar kind, even if the required resources are dwarfed by the price of complex conventional weapon systems.[68] Vulnerabilities have to be identified before they can be exploited; complex industrial systems need to be understood first; and a sophisticated attack vehicle may be so fine-tuned to one specific target configuration that a generic use may be difficult or impossible (consider a highly sophisticated rocket that can only be fired against one single target and at nothing else, even if some of its components may be reused).[69] What follows may be a new trend: the level of sophistication required to find an opportunity and to stage a successful cyber sabotage operation is rising. The better the protective and defensive setup of complex systems, the more sophistication, the more resources, the more skills, the more specificity in design, and the more organization is required from the attacker. Only very few sophisticated strategic actors may be able to pull off top-range computer sabotage operations.

The third conclusion is about defenses. The world's most sophisticated cyber forces have an interest in openness if they want to retain their edge, especially on the defensive. The precise offensive capabilities of the United States but also of other countries like Israel, France, China or North Korea are highly classified. There is much reason to assume that many spying operations are unknown to the victim. Even sabotage through logic bombs may have been already prepared without the knowledge of the defender. There may even be an incentive for governments as well as large firms to hide the true extent of cyber

[67]See for instance, Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation 2009), 32–3.

[68]Ralph Langner, 'A declaration of bankruptcy for US critical infrastructure protection', *The Last Line of Cyber Defense*, 3 June 2011.

[69]See Roberta Stempfley and Sean McGurk, *Testimony*, US House of Representatives, Committee on Energy and Commerce, 26 July 2011, 7, '[S]ophisticated malware of this type potentially has the ability to gain access to, steal detailed proprietary information from, and manipulate the systems that operate mission-critical processes within the nation's infrastructure.'

attacks, if they come to their attention, lest they would expose their vulnerabilities and damage their reputation as a place for secure investment. But cyber *defenses* of the most sophisticated countries should be more transparently presented. Only openness and oversight can expose and reduce weaknesses in organization, priorities, technology, and vision.

This article argued that the world never experienced an act of cyber war, which would have to be violent, instrumental, and – most importantly – politically attributed. No attack on record meets all of these criteria. Instead, the last decade saw increasingly sophisticated acts of network-enabled sabotage, espionage, and subversion. These activities can of course support military operations, and they have been used for that purpose for centuries. But the question is if a trend is leading to inevitable acts of stand-alone cyber war, with code as the main weapon, not as an auxiliary tool that is nice to have.

In the 1950s and 1960s, when Giraudoux was translated into English, the world faced another problem that many thought was inevitable: nuclear exchange. Herman Kahn, Bill Kaufmann, and Albert Wohlstetter were told that nuclear war could not be discussed publicly, as Richard Clarke pointed out in his alarmist book, *Cyber War*. He rightly concluded that as with nuclear security, there should be more public discussion on cyber security because so much of the work has been stamped secret. But in many ways the comparison between nuclear war and cyber conflict, although often made, is misplaced and problematic. This should be obvious when the Pearl Harbor comparison or the Hiroshima-analogy is given a second thought: unlike the nuclear theorists in the 1950s, cyber war theorists of the 2010s have never experienced the actual use of a deadly cyber weapon, let alone a devastating one like Little Boy. There was no and there is no Pearl Harbor of cyber war. Unless significantly more evidence and significantly more detail are presented publicly by more than one agency, we have to conclude that there will not be a Pearl Harbor of cyber war in the future either.[70] Then the heading of this article should not be understood with Giraudoux's sense of fine irony, but literally. Needless to say, Cassandra could still have the last word.

[70]In May 2011, the Obama White House stressed deterrence in cyberspace and made clear that 'certain hostile acts conducted through cyberspace' could trigger a military response by America (in using 'all necessary means', the document explicitly included military means). But the White House did not make clear what certain hostile acts (p. 14) or 'certain aggressive acts in cyberspace' (p. 10) actually mean, Barack Obama, *International Strategy for Cyberspace* (Washington, DC: White House, May 2011).

Acknowledgements

The author would like to thank David Betz, Peter McBurney, Tim Stevens and an anonymous reviewer for their helpful comments and the Institute for Advanced Study at Konstanz University for their support.

Notes on Contributor

Thomas Rid is a Reader in War Studies at King's College London and a non-resident fellow at the Center for Transatlantic Relations at the School for Advanced International Studies (SAIS), Johns Hopkins University, Washington, DC. In 2009/2010, Rid was a visiting scholar at the Hebrew University and the Shalem Center in Jerusalem. From 2006 to 2009 he worked at the Woodrow Wilson Center and the RAND Corporation in Washington, and at the Institut français des relations internationales in Paris. Rid published three books, *Understanding Counterinsurgency* (Routledge 2010, co-edited with Tom Keaney), *War 2.0* (Praeger 2009, with Marc Hecker) and *War and Media Operations* (Routledge 2007). More at http://thomasrid.org

Bibliography

Adair, Steven, 'Georgian Attacks: Remember Estonia?', *Shadow Server*, 13 Aug. 2008.

Adee, Sally, 'The Hunt for the Kill Switch', *IEEE Spectrum*, May 2008.

Arquilla, John and David Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy* 12/2 (1993), 141–65.

Arthur, Charles, 'William Hague reveals hacker attack on Foreign Office in call for cyber rules', *Guardian*, 6 Feb. 2011.

Blakely, Rhys, 'MI5 alert on China's cyberspace spy threat', *The Times*, 1 Dec. 2007.

Bright, Peter, 'Anonymous speaks: the inside story of the HBGary hack', *Ars Technica*, 15 Feb. 2011.

Broad, William J., John Markoff and David E. Sanger, 'Israeli test on worm called crucial in Iran nuclear delay', *New York Times*, 16 Jan. 2011, A1.

Carr, Jeffrey, 'Project Grey Goose Phase II Report', *GreyLogic*, 20 March 2009, Chapter 2.

Clarke, Richard A. and Robert K. Knake, *Cyber War* (New York: Ecco 2010).

Clausewitz, Carl von, *Vom Kriege* (Berlin: Ullstein 1832, 1980).

Clover, Charles, 'Kremlin-backed group behind Estonia cyber blitz', *Financial Times*, 11 March 2009.

Courtney, Siobhan, 'Pornographic videos flood YouTube', *BBC News*, 21 May 2009.

Crenshaw, Adrian, 'Crude, Inconsistent Threat: Understanding Anonymous', *Irongeek.com*, 28 March 2011, <http://bitly.com/e87PeA>.

Daniel, Lisa, 'Panetta: Intelligence Community Needs to Predict Uprisings', *American Forces Press Service*, 11 Feb. 2011.

Deibert, Ron and Rafal Rohozinsky, *Tracking Ghostnet* (Toronto: Munk Centre for International Studies 2009).

Dinstein, Yoram, 'Computer Network Attacks and Self-Defense', *International Law Studies* 76 (2002), 99–120.

Espiner, Tim, 'Estonia's cyberattacks: lessons learned, a year on', *ZDNet UK*, 1 May 2008.
Evron, Gadi, 'Battling Botnets and Online Mobs', *Science & Technology* (Winter/Spring 2008), 121–8.
Evron, Gadi, 'Authoritatively, Who was Behind the Estonian Attacks?' *Darkreading*, 17 March 2009.
Falliere, Nicolas, Liam O. Murchu and Eric Chien, *W32.Stuxnet Dossier. Version 1.4* (Symantec 2011).
Fulghum, David A., Robert Wall and Amy Butler, 'Cyber-Combat's First Shot', *Aviation Week & Space Technology* 167, 16 Nov. 2007, 28–31.
Fulghum, David A., Robert Wall and Amy Butler, 'Israel Shows Electronic Prowess', *Aviation Week & Space Technology* 168, 25 Nov. 2007.
Galula, David, *Counterinsurgency Warfare: Theory and Practice* (New York: Praeger 1964).
Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu and Phillip Laplante, 'Dimensions of Cyber Attacks', *IEEE Technology and Society Magazine* (Spring 2011), 28–38.
Gibbs, Jack P., 'Deterrence Theory and Research', in Gary Melton, Laura Nader and Richard A. Dienstbier (eds), *Law as a Behavioral Instrument* (Lincoln: Univ. of Nebraska Press 1986).
Giraudoux, Jean, *Tiger at the Gates [La Guerre De Troie N'aura Pas Lieu]*, translated by Christopher Fry (New York: Oxford University Press 1955).
Graham, Bradley, 'Hackers attack via Chinese web sites', *Washington Post*, 25 Aug. 2005.
Gross, Michael Joseph, 'A declaration of cyber-war', *Vanity Fair*, April 2011.
Hayden, Michael V., 'The Future of Things Cyber', *Strategic Studies Quarterly* 5/1 (Spring 2011), 3–7.
Langner, Ralph, 'What Stuxnet is All About', *The Last Line of Cyber Defense*, 10 Jan. 2011.
Langner, Ralph, 'Matching Langner's Stuxnet analysis and Symantec's dossier update', *The Last Line of Cyber Defense*, 21 Feb. 2011.
Langner, Ralph, 'Cracking Stuxnet', *TED Talk*, March 2011.
Langner, Ralph, 'A declaration of bankruptcy for US critical infrastructure protection', *The Last Line of Cyber Defense*, 3 June 2011.
Laqueur, Walter, *Guerrilla: A Historical and Critical Study* (Boston: Little, Brown 1976).
Libicki, Martin, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation 2009).
Lynn,William J., 'Defending a New Domain', *Foreign Affairs* 89/5 (2010), 97–108.
Mahnken, Thomas G., 'Cyber War and Cyber Warfare', in Kristin Lord and Travis Sharp (eds), *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. 2, (Washington, DC: CNAS 2011), 53–62.
Markoff, John, 'A silent attack, but not a subtle one', *New York Times*, 26 Sept. 2010.
Medetsky, Anatoly, 'KGB veteran denies CIA caused '82 blast', *Moscow Times*, 18 March 2004.
Nakashima, Ellen and Brian Krebs, 'Contractor blamed in DHS data breaches', *Washington Post*, 24 Sept. 2007, p.A1.
National Transportation Safety Board, 'Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999', Pipeline Accident Report NTSB/PAR-02/02 (Washington DC, 2002).
Nazario, Jose, 'Politically Motivated Denial of Service Attacks', in Christian Czosseck and Kenneth Geers (eds) *The Virtual Battlefield* (Amsterdam/Washington DC: IOS Press 2009), 163–81.
Obama, Barack, *International Strategy for Cyberspace* (Washington DC: White House, May 2011).
Ottis, Rain, 'From Pitchforks to Laptops: Volunteers in Cyber Conflicts', Conference on Cyber Conflict Proceedings (2010).
Reed, Thomas C., *At the Abyss* (New York: Random House 2004).

Rid, Thomas and Marc Hecker, 'The Terror Fringe', *Policy Review* 158 (December/Jan. 2010), 3–19.

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm and Liis Vihul, *Cyber Attacks against Georgia* (Tallinn: CCDCOE 2008).

Tikk, Eneken, Kadri Kaska and Liis Vihul, *International Cyber Incidents* (Tallinn: CCDCOE 2010).

Waxman, Matthew C., 'Cyber-Attacks and the Use of Force', *Yale Journal of International Law* 36 (2011), 421–59.