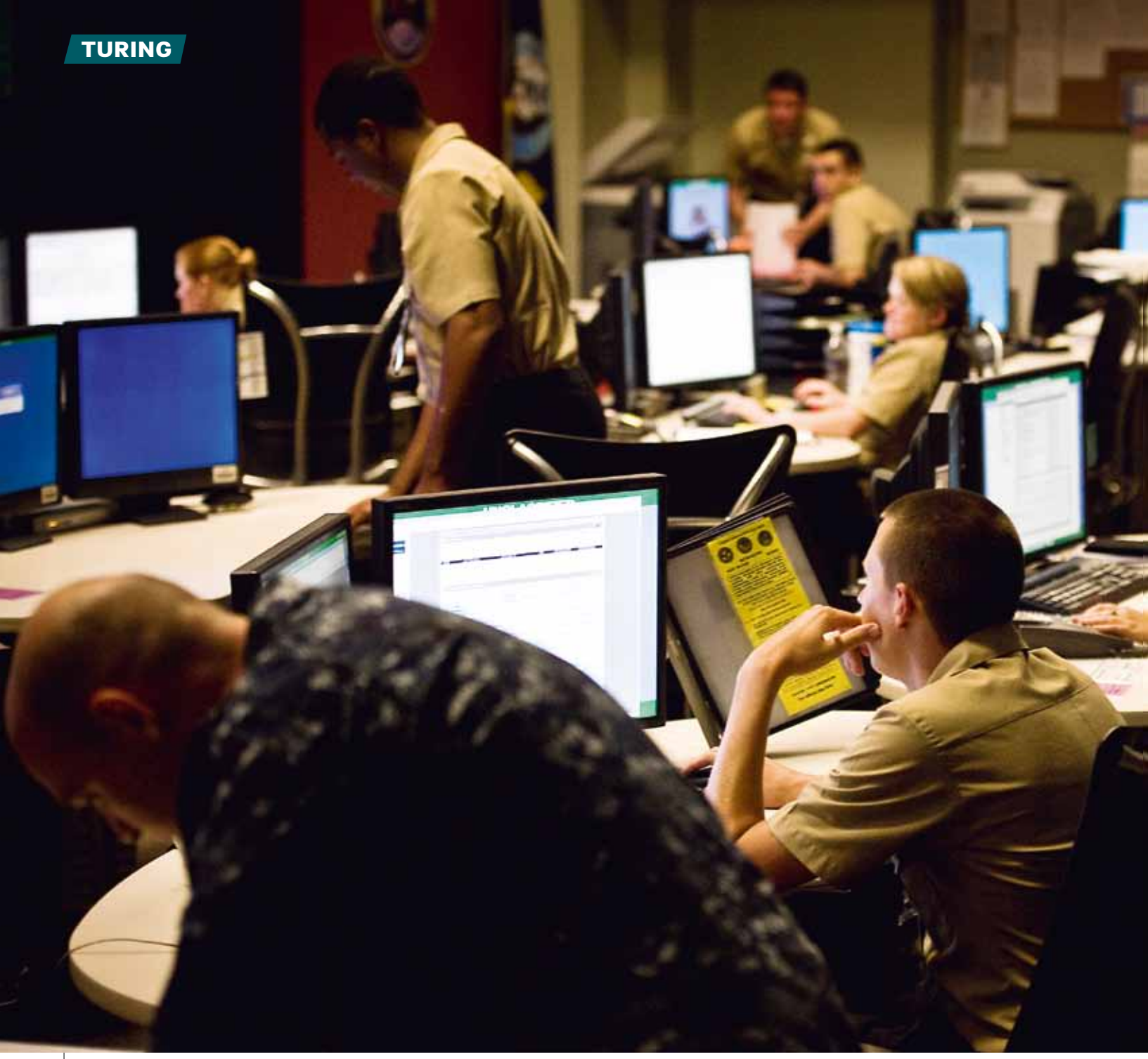

CYBER ACTIVE

Hardly a day goes by without the announcement of a significant computer hacking event, usually characterized as 'cyber warfare'. Typically, a company's computer system is breached and valuable data are stolen. Except that this is not cyber warfare, but merely a cyber-attack.

Rachel Marsden

Cyber operations in the United States military are now a truly joint affair with members of the US Navy, as pictured here, also staffing positions at the US DoD's Cyber Command © US Navy

Alongside kinetic combat, cyber warfare was utilized by both belligerents during the Russo-Georgian War of August 2008, including cyber attacks widely believed to have been perpetrated by Russia against Georgian targets online © US DoD

While hacktivists (individuals who subvert computers or computer networks often with a political goal in mind) operate by blocking a website's traffic with junk data in an attempt to render it unserviceable, this does not constitute an act of war. It is essentially a public relations act.

We very rarely hear about legitimate cyber warfare in the military context, which operates covertly in the shadows like the intelligence services and comprises the element of surprise employed by Special Operations Forces (SOF). The term 'cyber war' is nonetheless bandied about loosely in the public domain by media and government officials alike, without much effort made to differentiate between an attack on a computer system, and an act that constitutes actual war. So what exactly is the difference?

DEFINITIONS

Warfare is defined by international law and by the Geneva Conventions which comprises four treaties drafted in 1864, 1906, 1929 and 1949. The *Tallinn Manual*, published in April 2013, represents an attempt by the North Atlantic Treaty Organisation (NATO) Cooperative Cyber Defence Centre of Excellence based in Tallinn, Estonia, to fit cyber warfare within the parameters of international law as an extension of kinetic warfare. The manual defines the decorum of warfare in cyberspace and serves to explain why there has not been a catastrophic cyber event perpetrated on the civilian population of a country.

Chris Inglis, former deputy director of the United States National Security Agency which collects Signals Intelligence for the US government and now a strategic advisor to Securonix, a Los Angeles-based company that provides security threat intelligence to the private sector, argues that there should be decorum in cyber warfare: "Necessity and proportionality of response are conditioned by centuries of experienced practice. If someone attacks you with a pistol, it is not appropriate to shoot back with a cannon."

Therefore, what is and what is not permitted in cyber warfare? Cedric Pradel, a lecturer at the *Ecole de Guerre Economique* (Economic Warfare School) in Paris and a former French SOF cyber defence officer, says that cyber warfare can legitimately be used to gather intelligence; track an individual; perform psychological operations; neutralize an economic, political, communication, or social system; or sabotage a military system such as modifying the behaviour of a ground-based air surveillance radar to mask air strikes. Those drafting the *Tallinn Manual* concluded that Psychological Operations (PSYOPS), disinformation, or other 'ruses of war' do not meet the threshold for legitimate retaliatory cyber warfare. According to the *Tallinn Manual*, you cannot employ cyber warfare to cause injury or death to civilians, but you can proportionally target another country's military infrastructure and personnel as

Mindful of the threat posed to the interests of the United States and her allies, the US Department of Defence activated the country's Cyber Command in June 2009 © US DoD

Information operations comprise a host of capabilities including US Air Force aircraft such as Lockheed Martin EC-130H Compass Call electronic attack aircraft which may have already had cyber attack capabilities added to their repertoire © US DoD

well as any civilians participating directly in hostilities (such as mercenaries, for example), within the context of an ongoing conflict. Furthermore, cyber espionage is permitted, as long as it is not performed inside enemy territory. Being caught undertaking an act of cyber espionage on foreign soil could mean being treated in accordance with the laws of the land as they pertain to traditional spying.

Cyber espionage regarding companies has nothing to do with actual warfare or international law, according to the *Tallinn Manual*. Economic warfare has to be handled through diplomatic channels, by the judiciary and law enforcement organizations or through the imposition of economic sanctions. Those drafting the *Tallinn Manual* were divided on whether a single individual hacking catastrophically into a country's computer systems and networks could trigger a retaliatory attack. However, citing NATO and United Nations Security Council resolutions that followed in the wake of the 11 September 2001 *Al Qaeda* attacks against New York and Washington DC, they determined that a group of hackers outside of state direction could trigger a self-defensive counterattack if the initial hit was significant enough, in other words, if an attack caused serious harm to people, property or critical infrastructure. They also extended this provision to any attacks launched by Internet service providers or technology companies. "Nobody is very good at defence (as regards military cyber warfare)," says Mr. Inglis. "If this was a soccer game, the score would be 452 to 67, twenty minutes in. And any gap in offensive capabilities would close very quickly."

ATTRIBUTION

Attribution of attacks is another difficulty in the cyber realm of warfare. In conventional warfare between nations, attribution is straightforward, albeit less so when involving non-state or sub-state actors such as insurgent organizations, mercenaries or proxies . But cyberspace can take the chaos inherent in the 'Fog of War' defined by the Prussian military strategist Carl von Clausewitz to a whole new level. Even in cyber attacks on civilian targets, we very rarely see any actual technical proof of attribution. More commonly, we are simply told by a government or corporate official that the attack has been attributed to a nation-state and confidence and trust in their assessment is simply expected. Such was the case, for example, when Sony Pictures Entertainment's Hollywood office claimed to be the target of a cyber attack which consisted of the theft of communications and data in late November 2014. The attack was attributed to the Democratic People's Republic of Korea without any disclosed evidence to this effect, or even proof of whether the breach was an external one.

The risk of absence of reliable supporting technical evidence in attributing acts of military cyber warfare is far more serious than in the case of a company. Misattributed attacks in the cyber realm could be used by one nation against another as propaganda, or could result in misdirected retaliation. One of the companies producing technical analyses of cyber attacks as applicable to warfare is LookingGlass Cyber Solutions of Arlington, Virginia, which

has been monitoring a Russian state-sponsored cyber-espionage campaign active since at least mid-2013. LookingGlass's April 2015 report, *Operation Armageddon: Cyber Espionage as a Strategic Component of Modern Warfare*, details the targeting of Ukrainian government, law enforcement and military officials, ostensibly permitting insight into Ukrainian political and military strategies and plans. The firm's analysis provides a glimpse of how nations might engage in information warfare as an extension of modern kinetic warfare.

Wary of political subversion efforts, Russia viewed the sudden and substantial political unrest in neighbouring Ukraine resulting in the expulsion of its elected president, Viktor Yanukovych on 22 February 2014, as a threat to its own national security. Russia's military doctrine explicitly acknowledges information warfare as a legitimate component of war.

The Security Service of Ukraine (SSU), the country's domestic counter-intelligence agency attributed Russia's information warfare campaign to the 16th and 18th Centres of the Russian FSB domestic intelligence service. LookingGlass' findings support this attribution, says LookingGlass Chief Executive Officer (CEO) Chris Coleman, although he adds that this was not the focus of their investigation.

Mr. Coleman explains that "temporal analysis directly correlates waves of the campaign with physical conflict, even around ceasefire," that "multiple classified and internal documents were stolen and repurposed in waves of attacks using unsophisticated malware (malicious software)" and that the "SSU issued two public statements attributing the attacks to the Russian FSB, each time resulting in a change of (the latter's) tactics, techniques and procedures." LookingGlass' chief collection and intelligence officer, Jason Lewis, explains the role of cyber in warfare. "The first thing to know is that everything boils down to applying kinetic energy to a target. Intelligence is gathered to drop bombs on key targets. Intelligence is gathered to direct troop movements to supply depots. Intelligence is gathered to assist SOF in disrupting enemy communications ... Computer intelligence can assist in every scenario. The explosion of computing has made cyber intelligence more widespread, because of the proliferation of devices. Devices make everything faster and easier, so they are obvious targets."

COUNTERMEASURES

The tactics used in Russia's Ukraine campaign are not much different from those used by hackers against civilians for non-military purposes. According to LookingGlass' report, "Each attack in the campaign has started with a targeted spear phishing email convincing the victim to either open a malicious attachment or click a link leading to malicious content. The attackers use documents either previously stolen from or of high relevance and interest to Ukrainian targets, often government officials, in order to lure their victims into opening the malicious content." LookingGlass products can redirect clients away from known phishing sites to safe pages; for example, an IT (Information Technology) department page explaining why they are being redirected. Invicea of Fairfax, Virginia has a product that provides endpoint protection and attempts to intercept malicious attacks on each user's computer in the case of spear phishing. The final malware payload in the Russia/Ukraine campaign, in some cases buried in fake updates for Adobe Flash Player, Google Chrome or Internet Explorer software, is ultimately a Remote Administration Tool that allows an attacker access to the target's computer at will. Companies like California-based FireEye sell devices that can scan network traffic for these files and test their behaviour and quarantine them if they are classified as malicious. LookingGlass will prevent malware that has been activated from contacting command and control servers.

Philip Lieberman, president and CEO of Lieberman Software, develops products that help customers isolate and contain data breaches that occur after cyber attacks penetrate the network perimeter. "Much of the work in cyber defence is focused on understanding modern tradecraft and redesigning networks, identity management systems and privilege management to detect, thwart and/or slow down attackers. Much of the defence work is process driven and architectural; however, modern defences rely on modern technology that automates defensive responses and operate at rapid rates to minimize consequences." Mr. Lieberman also credits Microsoft and other 'cloud vendors' (a 'cloud' being a quaint term for the use of someone else's server as a data centre for storage of your own data) for developing and continually adapting cyber attack countermeasures: "The use of the cloud by both government and commercial (entities) represents some of the best hopes for society in that these organisations have the assets and knowledge to operate in a modern cyber warfare world."

Still, as Mr. Pradel points out, education is the first line of defence against any

The United States' National Security Agency is tasked with collecting communications intelligence. In recent years its work in this regard has been made public by the revelations of whistleblower Edward Snowden © NSA

Military personnel are employing cyber attack capabilities as part of their tool set for confronting and defeating an adversary during hostilities. The increasing use of the Internet as a propaganda and radicalization tool underlines how important such skills will be in the future © US DoD

such attacks. "In general we say that 90 percent of computer problems are between the chair and the keyboard, but in cyber security and cyber warfare the first line of defence is between the chair and the keyboard too." Simply not opening an email document attachment or link that looks inviting, or first verifying its legitimacy by other means prior to clicking on it, is the way to avoid being compromised.

THE FUTURE

The continued development of attack vectors is not likely to subside anytime soon. In December 2015, Google researchers reported that the quantum computer that it acquired, along with the US National Aeronautics and Space Administration and a consortium, from its Burnaby, Canada-based manufacturer, D-Wave, was 100 million times faster than a regular computer. This means that it is only a matter of time before conventional cryptographic algorithms can be cracked and supposedly protected data exposed in transit, due to the ability of such computers to perform high speed calculations.

None of this takes into account the backdoors already included within software as access points by intelligence agencies, a phenomenon brought to mass public awareness by the disclosures of former NSA contractor and CIA employee Edward Snowden in 2013. Whether or not those backdoors have now been closed has not been confirmed, but if an intelligence agency employs them for the purpose of information collection in the interests of national defence, then they also risk being found by malicious actors with less noble interests.

Despite its ongoing proliferation and a quiet cyber arms race, military cyber warfare is unlikely to result in the kind of catastrophic 'cyber Armageddon' as imagined by some. The result is likely to be much more insidious and drawn out. For example, the author recently disclosed exclusively in the *Chicago Tribune* group of client newspapers that a colleague, a former Master Sergeant in the US Army SOF, received a letter in November 2015 from the Office of Personnel Management (OPM) informing him that his personal information had been compromised in a data breach. Several of his colleagues received the same letter, which said that a "malicious cyber intrusion" had resulted in the theft of their background investigation files. These files contain the sort of sensitive personal information that must be disclosed to the government in order to obtain the highest level of US security clearance. When disclosing the attack earlier this year, government officials said the People's Republic of China was responsible, although this is impossible to prove since the access logs had been deleted by the time that the breach was discovered. What sort of personal information was stolen? According to the OPM's letter it included "name, Social Security number, address, date and place of birth, residency, educational and employment history, personal foreign travel history, information about immediate family members as well as business and personal acquaintances, and other information used to conduct and adjudicate your background investigation." These former service members have said that their files also include fingerprints, photos and information about vices and sensitive

As well as having implications for governments and corporations around the world, cyber warfare could also adversely affect the huge information-sharing networks which militaries now deploy into theatre to support operations © US Army

personal matters that could potentially be used for blackmail purposes. Some of the information dates back as far as 30 years.

The CIA was believed to be shielded from the data breach since it does not use the OPM for background investigations, but many SOF members end up working with the CIA on top-secret projects. It is unclear whether the personal information of current SOF members was stolen, but with so many former members working as contractors on classified projects, it is naive to suggest that the damage has been limited.

With fingerprints, photos and blackmail material, it is not difficult to imagine what a foreign government could do to compromise elite military operators. Personal vulnerabilities could be exploited to produce moles, with former military members blackmailed into spying or otherwise acting against national interests. For example, personnel suspected to be operating under deep cover in foreign territory could have a stray fingerprint lifted and checked against this rogue database in order to uncover their identity.

The exposure of information about family and friends provides malicious entities with easy entry into the lives of SOF personnel, since family and friends not trained in operational security themselves, are likely to be unsuspecting of any malicious agenda and likely have a ubiquitous Internet and social media presence. If they post details about family vacations on Facebook, Twitter or Instagram, hostile actors could ascertain the location of a top-secret operative.

What the attackers will actually do with the data remains unknown, but the victims are angrier with their own government and its demonstrated incompetence than with the perpetrators. "We talk a lot about a 'cyber Pearl Harbor,' this thunderclap that might go off some night, and there is a legitimate concern that there might be a sufficiently large attack on critical infrastructure, or sufficient failure through the vulnerabilities that are latent in some of these systems, that it is possible," says Mr. Inglis: "What I think is more likely is a sapping of corporate or governmental strength based on the insidious attacks that occur every hour of every day."

Subversion of a government through the slow erosion of citizens' confidence may very well end up being the most widespread visible result of cyber attacks, and this is not even tantamount to actual warfare, which is relegated to the shadows.