Information Operations Newsletter

Compiled by: **Mr. Jeff Harley**
US Army Space and Missile Defense Command
Army Forces Strategic Command
G39, Information Operations Division

ARSTRAT IO Newsletter on OSS.net

ARSTRAT IO Newsletter at Joint Training Integration Group for Information Operations (JTIG-IO) - Information Operations (IO) Training Portal

Table of Contents

Vol. 12, no. 06 (April 2012)

Al-Qaeda's Online Forums Go Dark for Extended Period

By Ellen Nakashima and Joby Warrick, Washington Post, April 2, 2012

Al-Qaeda's main Web forums have been offline for the past 11 days in what experts say is the longest sustained outage of the sites since they began operating eight years ago.

No one has publicly claimed responsibility for disabling the sites, but the breadth and the duration of the outages have prompted some experts to conclude the forums have been taken down in a cyberattack — launched perhaps by a government, government-backed organization or hacking group.

The first Web site, Shumukh al-Islam, a primary source for al-Qaeda videos and messages, went down on March 22, and since then four others have gone dark. The administrator of a second-tier al-Qaeda site recently posted a message on an online forum saying that "the media arena is witnessing a vicious attack by the cross and its helpers on the jihadi media castles."

Officials in the United States and elsewhere have long been concerned by sites associated with al-Qaeda. Those sites have been used to call for violence against Western targets and to try to recruit Islamic extremists to carry out attacks.

There remains uncertainty over whether the recent outages were caused by a cyberattack at all, and some skeptics note that some prominent al-Qaeda forums remain online. U.S. government agencies, including U.S. Cyber Command, had no role in the outages, according to officials who would speak about the issue only on condition of anonymity.

Still, Will McCants, a former State Department counterterrorism official who is now a senior fellow at the Homeland Security Policy Institute at George Washington University, said given the number of sites down and the duration of the outages, "it sure looks like a takedown."

If it were a technical problem being addressed by site administrators, "usually they will get on another site and say we've got administrative problems," McCants said.

The last lengthy blackout of al-Qaeda Web forums took place in the summer of 2010, when British intelligence officials disrupted the launch of an online magazine produced by the network's affiliate in Yemen.

In that case, the most prominent al-Qaeda site at the time, al Fallujah Web forum, was dark for at least seven days, said Evan Kohlmann, senior partner at Flashpoint Global Partners, which tracks the sites, which are mostly in Arabic language. The magazine appeared on the restored forum about two weeks later.

Although he generally sees the disruption of al-Qaeda Web sites as a fruitless game of whack-a-mole, Kohlmann said the most recent outages have clearly begun to affect jihadi communications.

"At least temporarily, the social networking among jihadists has been disrupted," he said. "The remaining forums are really struggling to attract the participation of users."

For years, U.S. intelligence officials have relied on al-Qaeda forums to gather insights into conversations among extremists. Some officials have argued against attempts to shut down the forums, saying they provide valuable intelligence.

At the same time, any cyberattack, even one that shut down an online forum only briefly, could temporarily stifle extremist activity, or perhaps just sow confusion and distrust among users.

Said one U.S. official: "It's a good thing whenever a terrorist Web site goes offline."

Regardless of the cause of the latest outages, if they persist, the larger consequences could be far-reaching, said A. Aaron Weisburd, a senior fellow at the Homeland Security Policy Institute who runs Internet Haganah, a site that tracks jihadi forums.

The loss of primary forums such as Shumukh and al-Fida' would deprive al-Qaeda of control over its message, he said. "It leaves the rank-and-file to guess which messages and which messengers are genuine al-Qaeda, and provides undercover operators with new opportunities to disrupt the movement," he said.

Comments on the handful of Arabic-language forums that remain online reflect the frustration and defiance among users.

"Life without Shumukh and Fida' is unbearable ... they are the Titanic supporting the foundation for the triumphant sects fighting in Iraq, Yemen, Somalia," a user identifying himself as Fata Musslim Ghayoor said on the Ansar al-Mujahideen Arabic Forum on Thursday, according to a Flashpoint translation.

"The forums will return," commented a user identified as "Azam" on a different site. "We are in a media battle with the enemies of Allah. ... Even if Shumukh is gone, a thousand other Shumukhs will be born."

Philip Mudd, a former longtime CIA and FBI counterterrorism expert, said he understands the intelligence value the sites have. But as the al-Qaeda movement loses ground, he said, "maybe the more important issue is how do we now get more aggressive in shutting down any effort they have to spread the message?"

In the past, U.S. officials have also relied on diplomatic channels to dismantle extremist sites that are seen as posing a threat to American personnel or interests, according to former U.S. officials familiar with the episodes.

The approach has worked in more than a dozen cases, and in each instance was backed by at least the implicit threat of a cyberattack by the U.S. military if the Web site's host country failed to act, the officials said. The countries that cooperated were in Europe, the Persian Gulf and the Pacific, they said.

"We've never had a country refuse us," said the former vice chairman of the Joint Chiefs of Staff, James Cartwright, speaking at U.S. China Commission hearing at George Mason University last week. "But if they did, then you can invoke the right of self-defense."

Cartwright said that in some cases the foreign government would be given a 48-hour window to investigate, what he termed "fair notice," before the U.S. military did so on its own.

The approach makes sense, current and former officials say. Although the U.S. government has the ability to disrupt the sites on its own, "you're not going to go do something unilaterally if you can do it cooperatively," said a former administration official who requested anonymity to discuss sensitive internal deliberations.

The al-Qaeda sites that have recently gone offline were hosted on servers in various countries, including Malaysia, Panama and the Gaza Strip, Kohlmann said. It is rare these days to see them hosted on servers in the United States or Canada, he said.

Some of the forum followers have suggested new outlets.

Said one commenter, Al-Muktafi bel-Lah, last week: "I suggest to the brothers having a page for the jihadi forums on Facebook and twitter."

Table of Contents

Debate Rages over Hacking Jihadist Websites

By Gary Thomas, VOA, 3 April 2012

Several al-Qaida chat rooms and forums, including its primary website Shumukah al-Islam, have been offline for several days in what experts believe was a coordinated cyberattack. Reports have speculated the action is the work of government intelligence agencies, which have been reluctant in the past to take down jihadist websites because they believe them to be a valuable source of information.

The debate continues in U.S. intelligence and policymaking circles about the value of attacking terrorist-group websites.

National security policy and information operations analyst Catherine Theohary, of the nonpartisan Congressional Research Service, said policymakers must weigh benefits against the cost in deciding whether to take down a terrorist group's website.

"There is an intelligence gain-loss calculus that takes place in deciding whether or not to take down a particular website because it could be used for monitoring and intel gathering, but also there could be a determination that, for whatever reason, a particular site may present a risk, an operational risk, to troops if it is actually being used to coordinate activities that could take place in real time," said Theohary.

Websites could provide clues to intelligence officers

Analysts say terrorist groups use the Internet to disseminate propaganda and pass orders. Jihadist chat rooms are gathering places for terrorists in cyberspace. Some would-be terrorists, such as the accused attacker in the 2009 massacre at Fort Hood, Texas, are reported to have drawn inspiration from the Internet.

Theohary said the websites, though, also may provide intelligence to counterterrorism officers.

"You can get a sense of following trends. It can be used to glean identities, to get a sense of upcoming operations that are being planned before they take place, things like that," she said.

Intelligence historian Matthew Aid said that in 2007 the Bush administration thought the Taliban was making propaganda gains on the Internet and wanted the group's websites shut down. But Aid said the intelligence community, led by the National Security Agency, strongly resisted.

"The intelligence community took the position that you can not take this stuff, you can not take these sites, down. We are learning more about the Taliban, their capabilities and intentions, by monitoring these sites than any possible advantage that could be derived from shutting them down. And the intelligence community prevailed on this point," said Aid.

Other analysts, however, differ. John Arquilla, a professor of defense analysis at the U.S. Naval Postgraduate School in California, said the intelligence gleaned from jihadist websites has been marginal. He believes random cyberattacks on the jihadist websites is a good tactic because they sow uncertainty among al-Qaida and like-minded groups.

"I want to take away the sense that the enemy has, that they have a virtual haven in cyberspace. I want them to worry that we are watching or listening. And on other occasions I want them to think that they are communicating securely when they are not. So we need to create doubt in their minds. We have given them far too much of a free ride in cyberspace," said Arquilla.

Analysts differ on who caused the outages

If the outages are the result of U.S. cyberattacks, the supersecret National Security Agency, which is the premier U.S. electronic intelligence body, is believed to be the agency that would do it.

But analysts believe an outside group could be responsible. Aid points out the technology to take down websites is not particularly difficult.

"The suggestion is that it is a U.S. government operation because it is comprehensive, meaning all of the sites are being attacked simultaneously and apparently very effectively, which suggests that somebody with a lot of technical know-how and wherewithal is doing it. But we live in a day when hacker groups like "Anonymous" have the exact same capability as the cyberwarriors up at Fort Meade, which is the NSA headquarters."

No one has claimed responsibility for the purported cyberattacks, though, and U.S. intelligence officials are refusing to comment on the matter

Table of Contents

Electric Dragons – Airborne Electronic Warfare Capabilities in China

By Robert Hewson, Royal United Services Institute, 29 Mar 2012

As an element of China's current air-power capabilities, electronic warfare (EW) assets appear to be less advanced than other key People's Liberation Army (PLA) air-combat systems, such as weapons and radars. However, the huge resources that have been devoted to military electronics in China are bearing fruit. Outside observers can now see two distinct EW competencies emerging within the PLA Air Force (PLAAF) – with the fielding of 'tactical' and 'strategic' frontline systems. China also has immense confidence in the domestic industry it has established to produce and develop the highly sophisticated hardware and software components that modern EW demands. However, one question remains unanswered: does all of this produce a combat capability that actually works?

The vast China Electronics Technology Group Corporation (CETC) and its many associated research institutes and manufacturing entities is at the core of China's EW industry. Conversations with CETC officials over the years have shown that they have a surprisingly deep understanding of Western EW systems – and how to counter them. China has also gained immense benefit from its extensive access to Russia's EW designers and manufacturers, whose business was sustained by Chinese orders over the long period when funding from Moscow dried up. Elsewhere, strong links are maintained with EW specialists in Ukraine – a country that plays an important part as a supplier of niche military technology, such as missile-seekers, to China.

China's modern era of airborne EW systems began with the acquisition of Sukhoi Su-27SK fighters from Russia in the early 1990s, along with their associated L-203 Gardenia wing-tip countermeasures pods. Later, the more advanced L-005 Sorbtsiya jamming system was acquired and carried by Su-30MKK strike fighters and late-model Su-27s (J-11A in PLAAF service). China is now building a developed, indigenised version of the Su-27 as the multi-role J-11B. These aircraft carry a podded EW system that closely resembles the Russian designs, but with several notable differences. An examination of the systems and subsystems that China has exhibited publicly shows airborne jammers that may be less powerful than their Russian equivalents, but with more modern and modular designs, based on the efficient integration of line-replaceable units. This approach should make these systems rapidly adaptable and upgradable – allowing them to better counter and defeat the threat systems that China expects to face.

A second key platform in China's tactical frontline force is the Xian JH-7 and JH-7A – the large, twin-engined strike fighter now emerging as the PLAAF's dedicated defence-suppression and electronic-attack aircraft. JH-7s and upgraded JH-7As have been observed operating with a suite of large, underwing jamming pods. Judging

from their size and configuration, each pod is dedicated to a different frequency range, indicating that the JH-7A could operate as an escort jammer (with a strike package) or a stand-alone electronic attack system.

The JH-7A has been integrated with a range of dedicated defence suppression weapons, including the YJ-91, China's version of the Russian Kh-31P (AS-17 'Krypton') high-speed, anti-radiation missile. A mix of armed and 'podded' JH-7As would make an effective US missile-seeking aircraft or 'Wild Weasel' defence-suppression team.

China's airborne EW systems will take another step forward once the enhanced Chengdu J-10B enters service. This much-improved version of the baseline J-10A will introduce the PLAAF's first electronic fighter radar (although it remains unclear whether it is a passive or active array design). This lays the groundwork for the potential use of such a large antenna system as an EW emitter. The J-10B also appears to have an integral EW system unlike any other found on a Chinese fighter, with a pair of jammers built into underwing hardpoints.

To feed this 'tactical' force of EW combat assets, the PLAAF has a modest, but active, fleet of 'strategic' electronic surveillance aircraft, the task of which is to collect the raw data needed to programme China's EW-threat libraries. These aircraft, known as Y-8JB, have been sighted on missions off the Japanese coast. A wide array of special-missions platforms has been developed from the venerable Shaanxi Y-8 four-engined turbo-prop. This includes a number of large, specialist EW platforms, such as the Y-8CB, Y-8G and others. Unlike the electronic intelligence-gathering Y-8JBs, these aircraft have a full-spectrum active EW mission and are part of China's expanding electronic-attack forces. The modernised and improved Y-9 platform will soon enter service and will provide a significant performance boost for future special-missions platforms.

China's military planners are well versed in concepts such as net- enabled and asymmetric warfare. At public events, the PLA had shown future combat scenarios that demonstrate a tight integration between its air, land and sea forces, using UAVs, guided weapons and electronic systems. The EW aspect of these plans is every bit as important as the kinetic aspect, which has been China's priority thus far. China has striven to reach an acceptable (near-peer) level of conventional military capability with land, sea and air platforms (eg tanks, ships and planes). Confident that this scenario has been achieved, China's military planners will focus on unconventional assets and improved combat support capabilities, all of which will call for the further expansion of an offensive EW force that is already on a solid foundation.

Table of Contents

'Azerbaijan Actively Joined Information Warfare'

From News.AZ, 04 April 2012

In recent year, the information warfare has become very important for our country.

Expert in media and PR technologies Ali Hajizade told the statement to Gun.Az while commenting on the informational propaganda of Azerbaijan.

"Azerbaijan has actively joined the information warfare, which involves state structures, different NGOs, media and individual citizens. Tangible achievements have been made in this direction. But besides these achievements, there a also a lot of shortcomings.

These shortcomings occur due to the incompetency of some of those involved in information warfare."

Table of Contents

Cyber War Will Not Take Place

By Thomas Rid, Journal of Strategic Studies, Volume 35, Issue 1, 2012

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.

*****

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 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]

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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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.

Notes

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

[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.

[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.

[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.

[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.

[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.

[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.

[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.

[28]Андрей Злобин, Ксения Болецкая, 'Электронная бомба,' *Ве омостu* [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.

[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.

[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 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.

[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.

[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.

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

[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.

[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.

[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.

[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>.

[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.

[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).

[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.'

[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).

Table of Contents

Designer Satellite Collisions from Covert Cyber War

By Jan Kallberg, Strategic Studies Quarterly, Spring 2012

Outer space has enjoyed two decades of fairly peaceful development since the Cold War, but once again it is becoming more competitive and contested, with increased militarization. Therefore, it is important the United States maintain its space superiority to ensure it has the capabilities required by modern warfare for successful operations. Today is different from earlier periods of space development,[1] because there is not a blatantly overt arms race in space,[2] but instead a covert challenge to US interests in maintaining superiority, resilience, and capability. A finite number of states consider themselves geopolitical actors; however, as long as the United States maintains space superiority, they must play according to a set of rules written without their consent and forced upon them. US space assets monitor the actions of authoritarian regimes and their pursuit of regional influence—a practice these regimes find quite disturbing. There- fore, any degradation or limitation of US space-borne capabilities would be seen as a successful outcome for such regimes. Cyber warfare offers these adversarial actors the opportunity to directly or indirectly destroy US space assets with minimal risk due to limited attribution and traceability. This article addresses how they might accomplish this objective. We must begin by examining US reliance on space before focusing on space clutter and the means an adversary might use to exploit it. While satellite protection is a challenge, there are several solutions the United States should consider in the years ahead.

US Reliance on Space

Network-centric warfare is dependent on the global information grid for joint war-fighting capabilities.[3] The pivotal layer creating global war-fighting capability is the space backbone of the information grid where space as- sets are the decisive element. The United States depends on space-borne capabilities for success, and US national security relies today on a limited number of heavily used satellites. These satellites are crucial for strategic deterrence, surveillance, intelligence gathering, and military communications. If strategic deterrence fails, the satellites become an integral part of offensive and defensive ballistic missile defense. Satellites are pivotal not only for American space superiority but also for information superiority—the engine in the multichannel joint war-fighting machinery that has proven to be successful in recent conflicts. American forces can fight globally be- cause of access to satellite-supported C4ISR. Potential adversaries of all sizes and intentions understand that American military might is closely linked to the capabilities of US space assets. James Finch and Shawn Steene of the Office of the Undersecretary of Defense for Policy express this unique link between space assets and national security well:

> Although other states increasingly utilize space for economic and military purposes, the United States is by far the most reliant on space systems due to its global responsibilities and high-technology approach to warfare that heavily leverages space systems for communication, navigation, and intelligence, surveillance, and reconnaissance. This asymmetry creates an imbalance; the more a nation relies on space systems, the more tempted a potential adversary is to target those systems.[4]

Since the fall of the Soviet Union, US space superiority has not been extensively challenged, and we have seen two decades of US space supremacy. At- tacks against US satellites have been a concern since the 1970s,[5] with a focus on signal jamming, laser beams from the earth,[6] and direct kinetic anti-satellite (ASAT) missile attacks. William J. Lynn III, former US deputy secretary of defense, stated in the summer of 2011,

> "The willingness of states to interfere with satellites in orbit has serious implications for our national security. Space systems enable our modern way of war. They allow our warfighters to strike with precision, to navigate with accuracy, to communicate with certainty, and to see the battlefield with clarity. Without them, many of our most important military advantages evaporate."[7]

Lynn's comments are to a high degree drawn from the *National Security Space Strategy* of January 2011. That strategy states that space is becoming congested, contested, and competitive. It clearly outlines the importance of protecting US space-borne capabilities:

> The *National Security Space Strategy* draws upon all elements of national power and requires active US leadership in space. The United States will pursue a set of interrelated strategic approaches to meet our national security space objectives: Promote responsible, peaceful, and safe use of space; provide improved US space capabilities; partner with

> responsible nations, international organizations, and commercial firms; prevent and deter aggression against space infrastructure that supports US national security; and prepare to defeat attacks and to operate in a degraded environment.[8]

Lynn also noted the impact of the growing amount of space debris:

> The specter of jamming is not the only new concern. The February 2009 col- lision of an Iridium communications satellite with a defunct Soviet satellite, and the earlier, deliberate destruction of a satellite by China, produced thousands of debris fragments, each of which poses a potentially catastrophic threat to operational spacecraft. In an instant, these events––one accidental, the other purposeful––doubled the amount of space debris, making space operations more complicated and dangerous.[9]

The deliberate kinetic attack and destruction of an outdated satellite by the Chinese themselves using an ASAT missile drew attention not only to the fact that the Chinese tested the missile and its policy impact[10] but also to the debris cloud the explosion created.

A Very Cluttered Space

The question of space debris is complicated by a myriad of issues involving not only the physical hurdles encountered in removing it but also legal and international issues.[11] As a result, space is becoming more congested, with around 1,100 active and 2,000 inactive satellites in orbit.[12] The amount of space debris has steadily increased over time,[13] with the total amount of debris currently tracked at 22,000 objects. The first steps to create a debris mitigation strategy were taken in the late 1970s.[14] Since then, thousands of satellites have been launched into space, and the majority of these are now either inactive or of an older technology generation and at the end of their life spans. The United States has led the debris reduction effort to mitigate risks by actively designing space vehicles that can be disposed of safely or removed by orbital decay.[15] The overriding concern regarding space debris is the mutual interest in limiting its effects and in creating a joint effort to decrease the amount of debris so that, eventually, orbital decay and gravity would prevail.

To understand the destructive power of space debris, one must consider velocity. A standard military-issue 5.56-mm round is traveling at 940 meters per second (m/sec.) when it leaves the barrel and can easily penetrate a human being. The US Army's 120-mm tank round has a muzzle velocity of 1,740 m/sec. and can pass through a medium-sized battle tank.[16] Space debris and space junk traveling at circular orbital speed will hit a satellite at speeds of from 3,000 m/sec. up to 7,600 m/sec., depending on altitude. Debris traveling up to eight times faster than a high-velocity rifle round— whether a long-lost monkey wrench from the 1970s stamped "CCCP," small fragments, or an intentionally dispersed steel ball—creates an unprecedented impact. Deliberately creating space debris in specific orbits can radically change the probabilities of impact, even if the majority of that debris were dispersed in various directions or removed by physical effects. A targeted collision or a large debris cloud in identical orbit would nullify the option to move the target out of the targeted area. Satellites are fragile masterpieces of electronics, cables, connectors, solar panels, integrated circuits, and high-frequency antennas. Every inch has a dedicated function. Any object traveling at 7,600 m/sec. is a real threat to a satellite.

The Kessler Syndrome

Former NASA expert on space debris, Donald J. Kessler, predicted the probability for collisions in space and the risk of a high amount of space debris being generated by the impact of a high-velocity collision.[17]

A chain reaction, called the Kessler Syndrome, could result. The Kessler Syndrome occurs when debris or another satellite hits a satellite or space junk with hypervelocity, creating a burst of more debris by the hypervelocity impact. If the satellite (or space junk) density is high enough, it can have a cascading effect through space. Kessler identified this problem but also clearly stated in the 1970s that the amount of space junk and satellites was too low to trigger such cascading effects and later reconfirmed that position. His contribution was to identify the potential problem and explain it. Since Kessler wrote about this phenomenon in 1978, he has returned to the topic to clarify, extend the question, or present his calculations.[18] Kessler's work is focused on unintended, random, and uncontrolled collisions. Similarly, the debate about space debris is focused on the unintentional creation of space debris by littering from space stations, exploding space boosters, and colliding objects.[19] In real terms—due to the limited probability for a random collision—the highest risk occurs with intended and premeditated creation of debris clouds that are concentrated around US mission-critical satellite orbits. If the collisions are intended, planned, and controlled, the risks are multiplied, presenting an adversary the opportunity to destroy pivotal US satellite hardware. To reach a cascading threshold, an adversary can add space debris through controlled and intentional actions. The fastest way to add space debris to an orbit is to collide the existing mass of satellites and space junk that orbits Earth. If the mass already in space can be hijacked through cyber attacks, the attacker minimizes its exposure to traceability and attribution.

Types and Means of Attack

Satellites are a major concern for any state or nonstate actor who intends to conduct operations in secrecy. Satellites gather intelligence, provide surveillance, and perform reconnaissance. This can be extremely annoying to states that seek to avoid transparency between their international commitments, their public posture, and their actions behind the scenes. Several options are available to those actors who seek to diminish this satellite threat.

Kinetic Attacks. Essentially, an adversary can choose between two types of noncyber anti-satellite attacks: direct kinetic and indirect kinetic. While a direct kinetic anti-satellite missile attack on a US satellite is possible, it would provide direct attribution to the attacker, thus leading to repercussions. The thruster and the heat from the missile would be identified and attributed to the country or vessel that launched the attack. A direct kinetic attack might be inviting, but the political price is high. Even though it would be inviting to attack satellites, an adversary would not be able to attack without leaving a trace of tangible evidence. Using an ASAT missile is a grave act of war and can only reasonably be used if the perpetrator anticipates and accepts a wartime response.

For a potential adversary, it can be far more advantageous to increase the amount of debris that clutters specific orbits, thus epitomizing the indirect attack. Increasing debris can be accomplished through actively adding debris to specific well-targeted orbits, systematic designer accidents, or collisions in space.

During the eighteenth century and until the Second World War, artillery units had a special round to be used if enemy infantry came uncomfortably close to the battery position—the case shot. The battery aimed toward the closing infantry and fired the case shots, which dispersed thousands of steel balls that created massive losses in the infantry ranks. Whether those steel balls hit an arm, a leg, the torso, or a hand did not matter; the infantry assault against the battery position lost momentum and ended. By applying the case shot idea to space, we can see an unsophisticated way to radically increase debris by using space boosters to reach lower Earth orbit (LEO) and then using kinetic energy to disperse hundreds of thousands of steel balls into a segment of space. Any obsolete or crude missile—exemplified by the Iranian Shahab or the North Korean Taepodong—could act as a space booster to take the payload to space. A salvo of 20 such crude space boosters delivering a significant amount of prefragmented shrapnel or steel balls could radically increase the amount of hypervelocity debris.

The probability for collision in space between a functional satellite and debris is a numbers game. Reduced to a simplified example, if the presence of 5,000 debris pieces at a specific altitude generates a risk of one satellite hit every 10 years—not taking into account additional debris generated from the impact—an additional 100,000 debris pieces would increase that risk drastically. To illustrate the principle, 20 space boosters can lift 30 metric tons of payload to LEO—roughly 400,000 steel balls—that would be spread at hypervelocity into the satellite orbits. The attack is kinetic but indirect, as the target satellites are not individually targeted but are instead approached by a swarm of hypervelocity debris that impacts the target satellites either by penetration or by destroying antennas, solar panels, or other equipment. This impact would initially generate more debris, although orbital decay would counterbalance some of it by moving it to a lower altitude; eventually it would disappear from space.

Either a direct or indirect kinetic attack would be an act of war and provide the necessary attribution to give the United States casus belli approved by at least a part of the international community. First, both the direct and in- direct kinetic attack would be attributable to the nation that launched the attack, and observations from space-borne monitoring satellites would be accurate enough to give the United States a solid case. Second, creating unprecedented amounts of space debris would not only be hazardous to US satellites but also to those of other major powers. If rogue nation X launches an indirect kinetic attack, it would affect Russia's, Europe's, China's, India's, Pakistan's, and other nations' satellites. Depending on the dispersement of these debris objects, damage could be limited to small areas of space, but it would still be a space territory not used solely by the United States. Rogue nation X traditionally has avoided United Nations–supported re-percussions from the international community when US interests have been damaged. Russia and/or China, in particular, are likely to veto any punitive actions proposed by the United States in the UN Security Council.[20]

In this scenario, rogue nation X cannot afford to lose that support by damaging Russian or Chinese space assets as collateral damage from its attack on US satellites. Chinese space assets are quite limited compared to Russian or US inventories; therefore, an indirect kinetic attack against US assets could result in severe damage to Chinese interests, as the Chinese lack space resilience. Neither direct nor indirect kinetic attacks are suitable or viable options for a rogue nation that intends to harm US satellites.

Cyber Attacks in Space. The life span of a satellite is between five and 30 years, and even afterward it can still be orbiting with enough propellant to move through space and with functional communications which could be reactivated. Space contains thousands of satellites, both active and inactive, launched by numerous

organizations and countries, hosting 5,000 space-borne transponders communicating with Earth. Every transmission is a potential inlet for a cyber attack. Older satellites share technological similarities, providing opportunities to cyber-exploit industrial systems for control and processing. Supervisory control and data acquisition (SCADA) systems within our municipalities, facilities, infrastructure, and factories are designed and built on older technology and hardware, sometimes designed decades ago, and the software is seldom updated. These SCADA systems are considered a strategic vulnerability and have drawn growing attention from the US cyber-defense community in recent years. Satellites may be based on hardware and technology from the 1980s for one very simple reason—they are unlikely to be upgraded after they have been launched into space.

Terrestrial cyber attacks are a single exploit on thousands, if not millions, of identical systems, and the exploit will be eliminated afterward by updates or upgrades. The difference between satellites and terrestrial cyber exploits is that a satellite is in many cases custom made, whereas the computing design is proprietary. Cyber attacks in space exploit a single system, or limited group of systems, within a larger group of satellites. These space-borne assets have a variety of operating systems, embedded software, and designs from disparate technological legacies. As more nations engage in launching satellites with a variety of technical sophistication, the risk for hijacking and manipulation through covert activity increases. A satellite's onboard computer (OBC) can allow reconfiguration and software updates, which increase its vulnerability to cyber attacks. A vulnerable satellite that will be orbiting for the next 10 years can be preset by a cyber perpetrator for unauthorized usage when needed.

Even with the most-advanced digital forensics tools, tracing a cyber attack is complicated on terrestrial computer systems, which are physically accessible. Space-borne systems do not allow physical access, thus, lack of access to the computer system nullifies several options for forensic evidence gathering. The only trace from the perpetrator is the actual transmissions and wireless attempts to penetrate the system. If these transmissions are not captured, the trace is lost.

If the adversary is skilled, it is more likely the attribution investigation will end with a set of spoofed innocent actors whose digital identities have been exploited in the attack rather than attribution to the real perpetrator. A strong suspicion would impact interstate relations, but full attribution and traceability are needed to create a case for reprisal and retaliation. Attribution can be graduated, and the level varies as to what would be accepted as an "attributed" attack. The national leadership can accept a lower level of tangible attribution, based on earlier intelligence reports and adversarial modus operandi, than the international community might demand, but it is restrained in taking action. China has had a growing interest in building cyber warfare capabilities [21] and is one of several nations that would have a sincere interest in degrading US space assets. Currently, nation-states are restrained by the political and economic repercussions of an attributed attack, but covert cyber war targeting US space assets removes the restraint of attribution.

A cyber attack resulting in a space collision would lack attribution and thus would be attractive to our covert adversaries. A collision between a suddenly moving foreign satellite and a mission-critical US satellite is neither a coincidence nor an accident. But without attribution, it does not matter that this is so obvious. Other forms of direct and indirect attack would be traceable to an attacker, which could result in military, economic, and political repercussions. In criminology we know that the major consideration of a perpetrator for premeditated acts is the risk of getting caught. The size of any repercussions if caught is secondary. If a cyber attack can destroy or disable US satellites with no attribution or traceability, it is likely to be considered by those who are openly adversaries and certainly by those who are covert. From a cyber warfare perspective, this creates an opportunity for a third party to hack and hijack a satellite with the express purpose of colliding with a mission-critical US satellite.

The attack could be either a direct collision or an indirect attack using the debris cloud from another collision. The ramming satellite can come from any country or international organization. The easiest way to perpetuate this attack would be to hijack satellites from countries less technically advanced or from less-protected or outdated systems.

The Hypervelocity Eight Ball. The term hypervelocity eight ball refers to the hitting of targeted satellites, directly or indirectly, with the intent to destroy the target by collision with hypervelocity objects. As previously discussed, the adversary can create a direct attack by ramming targeted US satellites with space vehicles through unauthorized cyber commands. The target for the initial step in an indirect attack may well be another satellite, part of a delivery vehicle, or space junk that will create significant debris upon impact. The collision creates hundreds or thousands of debris pieces that continue in space at high velocity. The debris cloud will affect other satellites in the collision orbit and may even initiate the Kessler Syndrome, causing proliferating damages if the threshold is reached.

Resolving the Space Challenge

While the problems and vulnerabilities in space and the means to attack space assets are significant, the United States does have options to mitigate these risks. The hypervelocity eight ball is more likely to occur if there are obsolete and inactive satellites abandoned in space that can be exploited for targeting and collision. Post-mission disposal (PMD),[22] the UN-initiated international effort to remove satellites after their productive life spans, would require satellites to be removed from space within 25 years[23] after their mission ends.[24] Naturally, it could happen earlier than 25 years, but it can also be a drawn-out process, as there are currently no tangible sanctions for noncompliance. If a satellite has a life span of 10–20 years, the additional 25-year allowance would increase the total number of years when the satellite can be remotely commanded to 35–45 years. Satellites launched in 1977, 1987, and 1997 are already technically outdated and several technology generations behind. The time between launch and end of operation for a satellite is the foundation for its cyber vulnerability. It is a sound financial decision to use a satellite to the full extent of its life span. But the question becomes Is it worth the risks? We must keep in mind technical leaps made since early space launches and what vulnerabilities could be embedded when space is populated by 25- to 45-year-old assets that can still navigate. Since technology today develops so quickly, PMD in reality increases the risk of cyber attack by hijacked satellites because it prolongs the time a satellite can be remotely commanded by radio signals exploiting obsolete and outdated communication equipment. The United States should propose shortening the PMD removal period and insist on communications updates to create secure control for all space assets.

If the peaceful and safe use of space is threatened, the United States will seek to deter and defeat aggression against space infrastructure. Preparedness to defeat attacks and operate in a degraded environment requires resilience—the ability to absorb loss of capacity while remaining operational. A single satellite can be used for intelligence gathering, all levels of military communications, and as a platform for different sensors. A specific type or design of satellite can be of critical importance and, therefore, a high-value target for adversaries to destroy. If a budget shortfall forces the United States to overutilize its satellites, it also increases the reliance on each individual satellite for war fighting and intelligence.[25] The obvious risk in an era of austerity is that budget cuts will prevail over resilience in pivotal space systems.

The 2010 National Space Policy requires us to "increase assurance and resilience of mission-essential functions enabled by commercial, civil, scientific, and national security spacecraft and supporting infrastructure against disruption, degradation, and destruction, whether from environmental, mechanical, electronic, or hostile causes."[26] Even in an era of federal austerity, it will be necessary to replace an aging fleet of US space assets because these assets are crucial for both commercial and national security functions. That would mean an increased number of satellites, even if the investment would create significant redundancy. This redundancy is a safeguard against the ability to operate in a degraded environment and provides vital resiliency.

Finally, the United States must adopt an active defense and probe the boundaries of cyber war in space. A limiting factor for success in defending space assets against cyber attack is regulatory constraints on information operations conducted by the DoD and related agencies. It is a policy decision that requires policy makers to understand the unique tenets of cyberspace. The unique character of cyber war will require easing restrictions on preemptive cyber warfare. If the United States can determine which satellites—active or inactive—can be used for designer collisions as a result of communication or navigational weaknesses, it can secure the disposal or safe removal of these vulnerabilities. By using active defenses, the United States increases its likelihood of detecting foreign countries trying to command satellite attacks.

The best way we can determine if the threat is real and if foreign space assets can be hijacked is to go out and try it ourselves—if only to determine possibilities. Assurance is not created by waiting for adversaries to execute their options and relying only on reactive incident response; instead, assurance requires mitigating the risks and determining the vulnerabilities. The only way to establish knowledge about foreign assets' vulnerabilities is to digitally probe their defenses. Taking an active defensive stand increases the opportunity to attribute and trace cyber attacks, which builds uncertainty among potential adversaries.

Conclusion

Attacking US satellites may well be a top priority for any potential or covert adversary, and the geopolitical benefit for successful covert attacks on US space assets is high. At the same time, the cost of entry into cyber warfare is low, which enables nation-states and nonstate actors that are unable to challenge US regional presence by conventional means to adapt and pursue unattributed cyber attacks against space assets to degrade US war-fighting ability.

Space assets are critical to the way the United States fights today, and it is likely the United States will be even more reliant on the use of space assets to maintain and defend information superiority in the foreseeable

future. The fact that adversaries have not attacked, tampered with, or destroyed US satellites does not affirm their intent not to.

Cyber attacks are traditionally one shot, because they exploit a vulnerability that can be eliminated afterward or corrected by newer technology. In reality, with 3,000 satellites—active and inactive—on-orbit, it is likely some are already staged to be hijacked if needed. Any adversary might exploit the opportunity provided by a vulnerable satellite that will be orbiting for the next 10 years. Cyber attack also offers the option for an adversary not already at war with the United States to damage US satellites covertly.

The best solution is active defense: gather information and probe the vulnerabilities of US and foreign satellites, build new satellites to replace aging US space assets, maintain the full military radio spectrum to ensure secure communications, and increase the number of satellites to ensure resilience in a degraded environment. Renewal and expansion of US space assets is critical for national security over the coming decades

NOTES

1. John Renaker, Dr. Strangelove and the Hideous Epoch: Deterrence in the Nuclear Age (Claremont, CA: Regina Books, 2000).

2. James Clay Moltz, The Politics of Space Security, 2nd ed. (Stanford, CA: Stanford Univer-

sity Press, 2011).

3. David S. Alberts, John J. Garstka, Richard E. Hayes, and David T. Signori, Understanding Information-Age Warfare (Washington: Command and Control Research Program Publication Series, 2001).

4. James P. Finch and Shawn Steene, "Finding Space in Deterrence: Toward a General Framework for 'Space Deterrence,' " Strategic Studies Quarterly 5, no. 4, (Winter 2011): 10–17. Finch and Steene are director and deputy director, respectively, of space policy and strategic development in the OSD-Policy.

5. "Soviet Arms Could Destroy U.S. Satellites, Brown Says," Baltimore Sun, 5 October 1977.

6. "Russian Laser 'Blinds' U.S. 'Spy Satellite', " Chicago Tribune, 22 November 1976.

7. William J. Lynn III, "A Military Strategy for the New Space Environment," Washington Quarterly 34, no. 3 (Summer 2011): 7–16.

8. Department of Defense, National Security Space Strategy, Unclassified Summary (Washington: DoD, January 2011), http://www.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.

9. Ibid.

10. Stefan A. Kaiser, "Viewpoint: Chinese Anti-Satellite Weapons: New Power Geometry and New Legal Policy," Astropolitics 6, no. 3 (Fall 2008): 313–23.

11. Andrew Brearley, "Faster than a Speeding Bullet: Orbital Debris," Astropolitics 3, no. 1 (Spring 2005): 1–34.

12. NASA, Orbital Debris Quarterly News 15, no. 4 (October 2011).

13. J. C. Liou and N. L. Johnson, "Risks in Space from Orbiting Debris," Science 311 (20 January 2006): 340–41.

14. Donald J. Kessler, "Sources of Orbital Debris and the Projected Environment for Future Spacecraft," AIAA International Meeting and Technology Display, AIAA-80-0855 (1980).

15. N. L. Johnson, "The Historical Effectiveness of Space Debris Mitigation Measures," International Space Review 11 (December 2005): 6–9.

16. American Ordinance, KEW/KEWA1/KEWA2 Sales Brochure, http://www.aollc.biz/pdf/120mmTankKEW.pdf.

17. Donald J. Kessler and Burton G. Cour-Palais, "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt," Journal of Geophysical Research 83 (1978): 63.

18. Donald J. Kessler, Nicholas L. Johnson, J. C. Liou, and Mark Matney, "The Kessler Syndrome: Implications to Future Space Operations," presentation to 33rd Annual AAS Guidance and Control Conference, 6–10 February 2010, Breckenridge, CO.

19. United Nations Office for Outer Space Affairs, Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space, http://orbitaldebris.jsc.nasa.gov/library/Space%20Debris%20Mitigation%20Guidelines_COPUOS.pdf.

20. "Russia and China Veto Draft Security Council Resolution on Syria, UN News Service," 4 October 2011, http://www.un.org/apps/news/story.asp?NewsID=39935&Cr=syria&Cr1=.

21. Kim Zetter, "Hackers Targeted U.S. Government Satellites," Wired, 27 October 2011, http://www.wired.com/threatlevel/2011/10/hackers-attack-satellites/.

22. P. H. Krisko, N. L. Johnson, and J. N. Opiela, "EVOLVE 4.0 Orbital Debris Mitigation Studies," Advances in Space Research 28, no. 9 (2001): 1385–90.

23. Nicholas L. Johnson, The Disposal of Spacecraft and Launch Vehicle Stages in Low Earth Orbit (Houston: NASA, 2007), http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20070021588_2007019149.pdf.

24. National Research Council Committee for the Assessment of NASA's Orbital Debris Programs, Limiting Future Collision Risk to Spacecraft: An Assessment of NASA's Meteoroid and Orbital Debris Programs (Washington: National Academies Press, 2011).

25. Office of the Undersecretary of Defense, National Defense Budget Estimates for FY 2012, http://comptroller.defense.gov/defbudget/fy2012/FY12_Green_Book.pdf.

26. National Space Policy of the United States of America (Washington: The White House, 2010), http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf.

Table of Contents

Al Hurra: An Eye on Democracy

By Jehad Saleh, Fikra Forum, March 28, 2012

When Al Hurra was launched in 2004, I was living in Syria amongst journalists and activists, fighting for freedom and human rights. With great conviction, we believed that this American channel would provide a platform for voices seeking freedom as well as an independent and daring media presence for those who were oppressed in countries lacking a free and independent press. Governments of these countries impose a culture of subordination and silence based on a general ideology that rejects change, freedom, and democracy, while supporting a single prevailing dominant culture.

In the beginning, Al Hurra succeeded in distinguishing itself with its unique programming and news broadcasting. While presenting a positive image of American culture and society to the Middle East, the U.S.

was portrayed as the ideal model of democracy and freedom with media that upholds freedom of expression and opinion. By harnessing these ideologies, Al Hurra intended to promote a culture of democracy, human freedoms, and monitoring human rights violations. In doing so, they were met with the countering ideas of authoritarian Arab regimes, who stated that Al Hurra promotes the U.S. agenda to overtake the Arab region. As enemies of democracy and transparency, intellectuals from the Arab regimes propagated this idea. Likewise, religious movements and political Islam spread the same message.

This article presents excerpts from an extensive report on the prospects of Al Hurra in the Middle East according to key voices from the region. This study aims to improve Al Hurra's performance in order to achieve its mission of democracy and human rights.

Culture of Tyrants

In the Middle East, accepting other's opinions and respecting opposing perspectives has not been a prevalent part of the culture. The culture of radicalism and authoritarianism has comprised a system which is limited to one narrow point of view that all people are expected to live by. All segments of society are condensed into a single template, whereby culture, intellectuals, and the media all stem from the authority of the person in power, the ruling family, or the military. Consequently, this creates major obstacles for the media that are difficult to break. Given the harsh punishment placed on free speech and democratic views, Al Hurra faced a wall of distorted culture.

How can Al Hurra overcome these obstacles? Writer George Kuten says that Al Hurra should be allowed to operate with more freedom and independence in order to properly convey its messages and gain a following. Writer Kefah Kareem believes that Al Hurra has fallen into the typical style of Arab media. However, journalist Amira Al-Tahawi highlights Al Hurra's good quality, with periodic coverage of issues concerning public freedoms, economic and social rights, sectarian demonstrations, and protests. Additionally, she spoke highly of the diversity of sources, which enrich the coverage with first-hand accounts rather than what is usually published by traditional media.

Al Hurra's Programming on Democracy and Human Rights

Al Hurra aims to reflect the humanitarian side of communities and the rights abuses they experience at the hand of regimes and individuals. Thus, the channel outrages governments and their state-sponsored media. Many hidden files, including prison records, torture methods, and cases of exiled individuals, have been exposed to the public, while the daily struggles of the people have been brought to light. Al Hurra also conveys the people's dreams of freedom and democracy.

In an interview with Syrian activist Ammar Abdulhamid, he suggests that Al Hurra adopts a liberal identity, acting as a platform for liberals:

"There are good programs with positive viewer reception like 'An Eye on Democracy,' however, these remain an exception. Al Hurra producers wanted to act as a competitor news network to Al Jazeera, Al Arabiya, and other news programs currently operating in official Arab media outlets. However, [Al Hurra was] unable to rely on a clear strategy or vision for the channel, coupled with multiple changes in their administrative structure. In addition, an unprecedented environment of competition was born due an increase in the number of Arabic language news channels with a variety of strategies and frameworks. The Arab citizen is inundated with many options, so unless the channel attracts the right audience and presents a clear perspective—the liberal one in particular—the channel will remain without an identity in an area that has no tolerance for ambiguity."

During its program "Free Hour," which is an hour-long program devoted to digesting and facing ongoing events in the region, Al Hurra aims to act as a platform for freedom. Despite its great value, the length of the program is insufficient.

Human rights activist Nael Georges Bunni believes that the channel needs to be a source of knowledge to promote a culture of human rights against all forms of tyranny, while addressing all types of regional issues.

Viewers complain about the channel's lack of depth into communities and their demands for freedom and democracy. Moreover, viewers don't think the channel meets a high enough standard, considering that it is being broadcasted from a democratic country where freedom of expression is sacred. They had hopes that the channel would serve as a mirror of transparency, reflecting the voices of the people in moments of darkness.

Minority issues

In the Middle East, many minority groups have greatly suffered, have been excluded, and have been denied basic rights under unjust systems that do not recognize their existence. Thus, minority issues have remained absent in Arab media. Al Hurra offers a window of light to minorities.

Novelist Fadila Farouk considers Al Hurra to be a high caliber channel of high quality and standards. She says: "The Arab public is young and exploited by the Islamic and authoritarian media. Al Hurra has to link itself to a

larger sector of society by touching on the problems of the Arab street and giving opportunities to real journalists who understand their communities in depth. The channel cannot be a voice for minorities like the Kurds & Amazighs simply because Arabic is the language of Arabs. In the Middle East, Al Hurra faces a hostile attitude toward Americans in general. Arab channels will not give way to an American channel to achieve success in their own backyard. Additionally, some of those responsible for dish cable networks shut down Al Hurra broadcasting according to the desires of certain political movements. This means that Al Hurra is confronting a public that is controlled by political movements that have no desire to understand the simple and gentle American person. If those struggling for freedom are distanced from Al Hurra, how can the concept of freedom and liberty spread amongst people and be promoted in such closed-off communities? People follow Al Manar day and night with non-stop exposure to religious channels during the day and sex channels at night."

Alternatively, rights activist Azad Diwani rejects the attitude of Al Hurra towards the Kurdish issue for its lack of coverage of human rights issues in the Kurdish regions of Syria, Iraq, Turkey, and Iran. The channel, he states, needs courageous cadres with a deep belief in the democratic rights of oppressed minorities and a willingness to build close ties with human rights defenders. However, there are some programs that deserve recognition such as "From Inside Washington: An Eye on Democracy," which is broadcast in Iraq and "Equality: the Documentary Hour." Furthermore, Azad adds that it is important to increase the number of episodes about American history and its democratic experience, which will attract more followers, particularly episodes that are aired in English with Arabic subtitles.

Al Hurra and the Arab Spring

As people in the Middle East rose up for freedom and democracy, we found Al Hurra competing with the media for coverage of the Tunisian and Egyptian revolutions, and trying to be the voice of the Syrian revolution. According to the Kurdish journalist Sirwan Kajjo, "Al Hurra was the leader in broadcasting accurate news, but remained captive to the traditional media. It lacked development and needed the professionalism of western news channels; however, it attracted journalists who were experienced in politics and civil issues."

Researcher Randa Kassis finds that the power of the media played a vital role in expressing revolutionary voices by exposing the democratic world to the reality of human suffering and the loss of basic rights to life and freedom. Randa states that "the media was like a mirror reflecting the revolutions of oppressed people, to the extent that it succeeded in breaking all taboos and putting an end to the culture that was upheld by tyrannical Arabs who viewed Arab dictators as eternal gods. While [Al Hurra] was considered a platform for revolutionaries, it did not position itself in the same way with regards to the Syrian revolution. In this case, the channel did not try to be the great media vessel of the revolution; instead, it contributed to the development of freedoms. It should overcome all obstacles in its way in order to be a channel for people aspiring for freedom by offering free and transparent programming. It should convey events according to the American media standards."

Al Hurra can succeed in creating free societies and an independent press and media if it bases its message on a humanitarian mission with transparency and boldness coupled with experienced journalists and press, while becoming the most watched channel in each house in the Middle East and the Arab world. Despite its faults, Al Hurra is an eye on democracy. However, people in the Middle East need it as their eyes to a broader range of words, images, and news stories. They need it to touch on their suffering with professionalism and credibility with more depth into the spirit of the communities that do not trust the politicized Arab media of regimes that are anti-democratic and against the freedom of expression.

Table of Contents

U.S. Navy Focus Shifts To Asia-Pacific

By David Fulghum, Aviation Week, 9 Apr 2012

The U.S. Navy's expanding mission in Asia and the Pacific Ocean is a striking example of early planning turned on its head by changing threats. That upset is now being righted by innovations on the fly.

New technologies—including aircraft carriers and stealthy strike aircraft—will be transferred to the Asia-Pacific theater. But equally new, foreign-built surveillance systems, electronic attack weapons and cyberinvasion tools are unexpectedly threatening crucial sensors and communications on advanced ships and aircraft, say top Pentagon officials.

The advanced F-35 Joint Strike Fighter, for example, has a new vulnerability. Its wide-angle field-of-view radar can be attacked with cyberweapons through its active, electronically scanned array (AESA) antennas. Airborne cyber-weapons form data beams that can be packed with malware and directed into a target

antenna. These devices are being developed by several nations specifically to electronically attack, jam, invade and exploit high-value, airborne targets, say U.S. electronic warfare (EW) specialists.

In particular, U.S. analysts have been watching China develop EW platforms to attack specific types of high-value sensor and command-and-control aircraft, says a longtime U.S. EW specialist. These include E-3 AWACS air-to-air radar, E-8 Joint Stars air-to-ground radar and P-8 maritime surveillance aircraft.

"Electronic attack can be the method of penetrating a system to implant viruses," says the EW specialist. "You've got to find a way into the workings of that [target] system and generally that's through some sort of emitted signal."

Moreover, three years ago, several terabytes of data—some of it related to the F-35's electronics systems—were copied during a series of break-ins of contractor networks. Penetrations were traced to known Chinese Internet addresses.

Part of the Navy's strategy is to shift at least one additional, new-built aircraft carrier—packed with AESA-equipped aircraft—to the West Coast for duty in the Pacific. The new carrier designs have added aircraft elevators and centralized weapons lifts to increase the speed of rearming and sortie generation by 25%, says Rear Adm. Thomas Moore, the Navy's program executive officer for aircraft carriers.

But Rep. Adam Smith (D-Wash.), ranking member of the House Armed Services Committee, has noted the "constantly evolving and changing" cyber-threat.

In fact, the potential problem threatens the advanced radar on all models of the F-35, F/A-18 Super Hornet and EA-18G Growler. Each has an AESA that doubles or triples the radar's resolution and ranges over conventional radio-frequency sensors. The radars also are adept at collecting signals that can be altered and infected.

"I'm particularly worried about the effects of jammers [and cyberattack] on our radars," says Deputy Defense Secretary Ashton Carter. "It's difficult to separate electronic warfare from cyberattack. EW is an area that is under-valued and understressed. In some places we've fallen behind."

As a result, initiatives are being launched to block those radar vulnerabilities. Last summer, specialists started combing through the Pentagon's EW programs and will decide this fall where to allocate additional funds to catch up, says Carter. Specialists know a lot about EW and cyberoperations as applied in Iran and Afghanistan, but now the Air Force and Navy are looking at the more formidable technologies they will face in the Asia-Pacific region. So far, most of the upgrades for tactical aircraft and shipboard radars to counter jammers and cyberattacks have been sustained in the proposed 2013 budget. But cuts will still impact EW and cyber programs.

"We're still not remotely satisfied with cyber [defenses]," says Carter. "We have several different projects . . . to secure military networks and to provide network support for the civilian infrastructure. When it comes to cyber, we're not only protecting but actually increasing a lot of the new capabilities."

The veteran airborne EW specialist says the threat to radars and other systems using AESA antennas is less a looming catastrophe than simply another thrust and parry in the fencing match of EW that has been going on since before World War II. "As radars mature, the signals processing gets smarter and intrusion becomes less of an issue until some new technique is invented," he says. "The benefit of our new systems is that they have multiple sensors covering different parts of the electromagnetic spectrum that -allow sensor fusion to overcome point solutions with digital RF memory and tremendous signal processing capability."

As for whether an AESA could serve as a conduit for EW or cyberattack, the same issue surrounds any other electronic aperture on an aircraft, ship or vehicle. In fact, AESAs have had to deal with jamming and spoofing from the beginning of their use. The first F-22 squadron, for example, had its sensitive electronic surveillance overwhelmed by large radars on ships from the nearby Norfolk, Va., naval base.

"The only new issue is the attempted introduction of a virus or some other network attack element through the AESA," says the EW specialist. "All are conduits for incoming signals. The question is how you process the signal to retain the value-added information and reject or exploit the hostile content. As in most systems, we have multiple layers of signals rejection."

There are ways to attack an AESA radar on a dedicated one-to-one basis, says Lt. Gen. Herbert Carlisle, the Air Force's deputy chief of staff for operations. However, that vulnerability can be mitigated by the fusion of multiple radars. If several aircraft with -AESAs network themselves together, the radar being attacked can shut down and rely on information available on the network. Another option is to switch to infrared or electro-optical sensors.

"There is a technique we are looking at that involves sensor fusion combined with a network-integrated capability to take data from multiple sources as a defense," Carlisle says.

Table of Contents

What does #NTVlies Really Mean?

David J. Smith, Potomac Institute for Policy Studies, Tabula, April 9 – 15, 2012

#нтвлжет—#ntvlies—is the latest online rallying point for the persistent opposition to Russian President-elect Vladimir Vladimirovich Putin. The immediate object of the protest is the NTV television documentary Anatomy of a Protest, a "pseudodocumentary," writes the New York Times, with "all the familiar earmarks of a hatchet job against opponents of the Kremlin." On a deeper level, #нтвлжет signifies that some segment of the Russian people is unwilling to leave behind Putin's tragicomic Kremlin re-entry. Their web-based protest against the Gazprom-owned television channel marks Russia's transition from broadcast to online politics.

In a September 2011 Washington Post article, American author Ralph Peters remarks that "Putin's genius…begins with an insight into governance that eluded the 'great' dictators of the last century: you need control only public life, not personal lives. Putin grasped that human beings need to let off steam about the world's ills, and that letting them do so around the kitchen table, over a bottle of vodka, does no harm to the state. His tacit compact with the Russian people is that they may do or say what they like behind closed doors, as long as they don't take it into the streets."

At that time, it appeared that the siloviki understood that the Runet—as the Russian segment of the Internet is called—is more like a virtual street than a virtual kitchen table. People can let off steam on social media and blog sites, but they can also persuade, multiply and organize.

(Siloviki, literally people of force or power, is a slang term applied to current and former members of the Russian security services who are the dominant faction in Putin's government.)

"Uncontrolled usage [of the Runet]," FSB Cyber Center Chief Alexander Andreyechkin warned last spring, "may lead to a massive threat to Russia's security."

The Kremlin had one eye on social media-driven events abroad. "Look at the situation that has unfolded in the Middle East and the Arab world," said President Dmitry Medvedev. "This is the kind of scenario that they were preparing for us, and now they will be trying even harder to bring it about."

But the Kremlin's other eye was focused on the Duma and presidential elections upcoming in late 2011 and early 2012. In what could only have been a trial run before the elections, during March and April 2011, the now-familiar crew of youth group and criminal hackers launched a series of DDoS attacks on the LiveJournal blog site, Novaya Gazeta newspaper website and Rospil.info, a website run by anti-corruption blogger Aleksey Navalny.

(DDoS attacks come from hundreds, maybe thousands of computers herded without their owners' knowledge into a botnet. Upon command of the so-called botherder, each computer in the botnet blasts requests at the target website until it is overwhelmed and unable to perform its intended function.)

"Hardly anyone could have done this other than the security services," said People's Freedom Party leader Boris Nemtsov. The spring 2011 attacks were warnings to Russian Internet denizens that the Runet is carefully observed.

On the occasion of the December 4 Duma elections, as expected, DDoS attacks were aimed at about 30 websites more or less identified with the opposition. Among the attacked sites were LiveJournal, news portals slon.ru, Zaks.ru, Novaya Gazeta, New Times and Kommersant newspapers, Bolshoi Gorod magazine, Echo Moskvy radio and TV channel Dozhd. Election watchdog Golos also came under cyber fire, particularly its Kartanarusheniy.ru, a project to display election violations on an interactive map.

However, the gravity of the matter expressed by the siloviki a few months earlier was not reflected in the December efforts to suppress online opposition. Some sites were taken down, but one could read about it on other sites. And while browsing the available sites, one might have found an amateur video of ballot box stuffing at some or other polling station. One got the impression that the siloviki and their hacker friends did not comprehend the extent of the Runet challenge.

Having successfully employed social media to reveal election irregularities, the wired opposition then used the same means to bring hundreds of thousands of people into the streets of cities across Russia.

Putin appeared dazed. Ten days after the election, during his annual television call-in program, he ridiculed the white ribbons worn by street protestors. "Frankly," he said, "when I looked at the television screen and saw something hanging from someone's chest, honestly, it's indecent, but I decided that it was propaganda to fight Aids—that they had hung, pardon, a condom."

Meanwhile, looking forward to the March 4 presidential election, the Putin camp decided to join the Internet era with a slick "Vladimir Putin 2012" website. The home page featured a vigorous-looking sports shirt-clad Putin against a snowy backdrop. The content included an essay about why he should be Russia's president.

However, the Putin people apparently mistook a computer screen for a television screen. Television broadcasts one way; on the Internet, people talk back. The only thing they could think to do with the torrent of negative comments was to delete them.

Nonetheless, the vast majority of the Russian people still gets most of its information from television, and Putin handily won the March 4 election, (from which any serious opposition had been carefully excised months earlier).

In March, DDoS attacks—at least on an appreciable scale—did not materialize. Perhaps, buoyed by favorable pre-election polls, the Putin people decided that good, old-fashioned ballot box stuffing would suffice. Perhaps embarrassed at home and abroad by the December 4 DDoS debacle, they decided to reconsider and revamp their cyber capabilities. Whatever the reason, it is interesting that the perpetrators—who some continue to believe are spontaneous cyber patriots—could be called off so efficiently, with the snap of someone's fingers.

They will be back. But, for now, the wired opposition persists—#нтвлжет is just their latest iteration. Likewise, the system persists with broadcast politics like the Anatomy of a Protest documentary. However, there is a new factor. Like Putin's website, NTV's program became interactive—not directly, of course, but online comments about the television program and online protest organization rendered NTV, for a brief period, interactive. And the Russian faction of the hacker group Anonymous even launched a DDoS attack on the station's website, bringing it down for eleven hours.

With half of Russians already connected to the Internet, and 10,000 people joining each day, politics is moving online. That alone will make Vladimir Vladimirovich's third presidency very different from his first two.

Table of Contents

Global Briefing: Russian Politics Moves Online

By Khatuna Mshvidobadze, Jewish Institute for National Security Affairs, March 27, 2012

Social media today is becoming such a powerful political force that it might be called the fifth estate. And that fifth estate played an important role in Russia during the run up to the March 4 elections for that country's parliament and presidency. Georgians-who sustained combined Russian kinetic and cyber attacks in 2008-watched with more than passing interest. The Putin regime, it seems, turned some of the cyber techniques employed against Georgia against its own domestic opposition. The Kremlin openly wondered whether the Runet-as the Russian portion of the Internet is called-could become the fuse that ignited a Russian autumn to match the so-called Arab Spring.

"Look at the situation that has unfolded in the Middle East and the Arab world," Russian President Dmitry Medvedev told the National Antiterrorist Committee in February 2011. "It is extremely bad. There are major difficulties ahead...We need to look the truth in the eyes. This is the kind of scenario that they were preparing for us, and now they will be trying even harder to bring it about."

Soon after Medvedev's lament, Prosecutor General Yuri Chaika told his CIS counterparts, "You saw what happened in London...In my opinion, the problem is evident and we need to bring social networks under reasonable control-simply to protect citizens' freedoms."

The Moscow political establishment-or some portions of it, at least-appeared alarmed as elections loomed. Why? Because Russia has become the biggest user in Europe and Internet penetration is also increasing. According to the Russian Ministry of Communications, in 2011, 70 million people were connected to the Internet, of whom 80% were active users. By 2013, the Runet could have more than 90 million users.

And these figures are largely driven by the popularity of social media in Russia. For example, Vkontakte, Russia's most famous social network, has a daily audience of 30 million. And the Live Journal blog site is also immensely popular. In Russia, these two dwarf Facebook and Twitter. This growing phenomenon has international and domestic consequences.

With so many people equipped to hear "dangerous" ideas, one can imagine that the Russian government is anxious to protect its people against infection from abroad. Consequently, Russian diplomats have been pushing around the United Nations General Assembly a warmed over version of a Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security.

The core idea of the agreement is to outlaw the broadcast by mass media or across the Internet of any information that could "distort the perception of the political system, social order, domestic and foreign policy, important political and social processes in the state, spiritual, moral and cultural values of its citizens."

So far, the idea has not gained much traction. As we have seen over the last year or so, however, most ideas that the Kremlin considers dangerous originate not across the world, but across town. In the run-up to the recent elections, social media became the platforms for political consciousness, discussion and even battle. It was unsurprising, therefore, to see that unique Russian nexus of external aggression, internal repression, cyber-crime and government turn its attention to the Runet.

Russian opposition figures, political bloggers and independent media have been sporadically targeted for some time. During March and April 2011, however, intermittent cyber waves swelled into a typhoon of Distributed Denial of Service Attacks (DDoS). (DDoS attacks come from hundreds, maybe thousands of computers herded without their owners' knowledge into a botnet. Upon command of the so-called botherder, each computer in the botnet blasts requests at the target website until it is overwhelmed and unable to perform its intended function.)

In March and April 2011, massive DDoS attacks were directed at LiveJournal and Novaya Gazeta, a newspaper that covers political and social affairs. It is best known for its murdered journalist Anna Politkovskaya, who was gunned down in the elevator of her apartment building as she was about to file a story on Russian security forces' misconduct in Chechnya.

Novaya Gazeta's project at the time of the spring 2011 attack was to launch "Online Parliament of Runet." The idea was to crowd-source nominations and then conduct "elections" for a parallel online Duma. Elected members would then blog about issues that, in their view, the government wants to avoid.

During the same period, Boris Nemtsov, former governor of Nizhny Novgorod and People's Freedom Party leader, had planned to publish a new report, "Putin. Corruption," on LiveJournal.

"DDoS-attacks, hacking blogs and e-mails-it's their old, common business," commented Anton Nosik, social media observer and a director at Live Journal's parent company, on snob.ru. "At first glance," he continued, "just look whom our elusive and omnipresent cyber crime targeted over the years and then the main principle of this list will be clear. We will see in it web sites of Georgian and Estonian government agencies, servers of Komersant and Gazeta.ru and opposition blogs."

"Hardly anyone could have done this other than the security services," said Nemtsov. The spring cyber typhoon was a warning signal sent to Russia's Internet generation that the Runet is carefully observed, precisely because, as Nemtsov said, it had become "truly a territory of freedom and this is a preparation for parliamentary and presidential elections."

Ironically, the Russian authorities had a hand in developing social media as the fifth estate. Due to media censorship and intimidation, the Runet became the vehicle for domestic opposition and emerging political figures. For example, Alexey Navalniy, the most recognized leader of the recent anti-Putin demonstrations, never had opportunities to appear on television. He literally emerged as a public figure from his anti-corruption blog on LiveJournal and his Rospil.info web site that monitors state procurement.

As predicted, apparently the same cyber forces were at work for the December 4 State Duma elections. DDoS attacks brought down LiveJournal and Novaya Gazeta, news portals slon.ru and Zaks.ru, New Times and Kommersant newspapers, Bolshoi Gorod magazine, Echo Moskvy radio and many more.

In a similar vein, right after the Duma election, Pavel Durov, Vkontakte General Director, received an official letter from the FSB-successor to the infamous KGB-to shut down particular Vkontakte political groups. Durov not only rejected the request, but he scanned the letter and posted it on the Internet.

Remarkable is that, despite publicly expressed concerns from the security forces, an apparent trial run and a significant DDoS effort on election day, the perpetrators failed to understand the nature of the Internet. One could read on one site that another site had been attacked. And, incidentally, one could view there an amateur video of ballot stuffing at some or other polling station.

The resultant mass demonstrations sent the regime reeling. Putin stonewalled opposition demands for a new election, conceding only that web cameras should be installed in 90,000 polling stations for the March 4 presidential elections.

Cyber attacks did not materialize during the presidential election, but some of the 90,000 webcams displayed fraudsters at work. If you missed the live stream on webvybory2012.ru, the images were flashed around the Internet in the form of thousands of videos, pictures, blogs, micro blogs and updates discussing, debating and condemning the March 4 process. The Runet really became the Russian political arena, the dawn of fifth estate in Russian politics.

A combination of real votes, traditional media control and old-fashioned electoral shenanigans was sufficient to elect Vladimir Putin as Russia's next president. The presidency to which he has been elected, however, will be very different from his two earlier ones, not least because politics are shifting to the Runet.

The cyber criminals and youth hacktivists were apparently called off on this occasion. But just as sure as political opponents will continue to express themselves and organize on the Runet, particularly on social media sites, we can expect to see their cyber foes back in action. Moreover, it would be foolish to think that the same people who designed Russia's cyber-attack on Georgia and its own domestic opposition are not busy building trap doors and laying logic bombs in the information systems of Russia's prospective enemies.

Table of Contents

Zombie Followers and Fake Re-Tweets

From The Economist, Mar 17th 2012

IN THE year 15AD, during the short-lived Xin dynasty, a rumour spread that a yellow dragon, a symbol of the emperor, had inauspiciously crashed into a temple in the mountains of central China and died. Ten thousand people rushed to the site. The emperor Wang Mang, aggrieved by such seditious gossip, ordered arrests and interrogations to quash the rumour, but never found the source. He was dethroned and killed eight years later, and Han-dynasty rule was restored.

The next ruler, Emperor Guangwu, took a different approach, studying rumours as a barometer of public sentiment, according to a recent book "Rumours in the Han Dynasty" by Lu Zongli, a historian. Guangwu's government compiled a "Rumours Report", cataloguing people's complaints about local officials, and making assessments that were passed to the emperor. The early Eastern Han dynasty became known for officials who were less corrupt and more attuned to the people.

Modern China's Communist Party rulers make use of both these methods in the era of microblogs, or weibo, the various Chinese equivalents of Twitter, which is blocked in China. It is hard to overestimate how much the arrival of weibo has changed the dynamic between rulers and ruled over the past two years. More than 250m Chinese internet users have taken to microblogs for many purposes, plenty of them purely recreational. But a popular pastime is to spread news and rumours, both true and false, that challenge the official script of government officials and state-propaganda organs.

The authorities have responded in two main ways. One has been to increase their own use of weibo as a listening post, a strain of governance in the spirit of Emperor Guangwu; the other, more in the spirit of the dethroned Wang Mang, has been to combat rumours harshly and to tighten controls over the microblogs and their users, censoring posts and closely monitoring troublemakers. Officials are attempting to make these tasks more manageable by requiring that users of the most prominent microblog service, Sina Weibo, register using their real name and identity-card number by March 16th. The other leading microblog, called Tencent Weibo, now also requires new users to register with their real name. Microbloggers can continue using nicknames as their online identities, as long as the weibo providers have their real-world identities on file.

It is unclear how much the real-name requirement will affect what microbloggers say. Indeed, it remains unclear how strictly it will be enforced, considering the booming market that already exists in microblog-related trickery. For mere pennies you can buy followers for your weibo account to make you look more popular (known as "zombie followers" because they mindlessly follow others). You can also purchase re-tweets and even comments on your posts. Inevitably amid all this enterprise, some companies say that for a fee (of around $80), they can provide official verification for weibo accounts, apparently allowing customers to register under fake identities (the microblogs verify legitimate users for nothing).

No matter how it is enforced, user verification seems unlikely to deter the spread of rumours and information that has so concerned authorities. Aware that they cannot ignore this new outlet for public opinion, officials have moved to engage with it: government agencies, party organs and individual officials have set up more than 50,000 weibo accounts, according to the Chinese Academy of Governance.

This degree of online engagement can be awkward for authorities used to a comfortable buffer from public opinion. When Wang Lijun, the former police chief of the region of Chongqing, sought shelter at an American consulate last month, the story broke fast on microblogs. Responding to the online frenzy, a Chongqing government weibo account claimed that Mr Wang was on medical leave receiving "vacation-style treatment", a comically implausible euphemism that immediately went viral. The news on March 15th that Mr Wang's erstwhile patron, Bo Xilai, had been sacked as party secretary of Chongqing marked the first time a high-level purge has been commented on in real time by microbloggers.

Authorities keep a close eye on online troublemakers, but rely on internet companies to fence and supervise their own playgrounds. The big microblogs employ hundreds of monitors to remove content they know will be unacceptable to the authorities. Yet the task of quashing rumours is a Sisyphean one. Rumours can run especially rampant in China because, even as citizens now have more social space in which to live, the country

lacks sufficiently reliable institutions, such as an independent press and judiciary, to play the role of referee. It is left to officials and the state media to implore netizens to be responsible.

Who you gonna call ?

In this task, officialdom has some allies. One is Dianzizheng, the online alias of a 43-year-old rumour-hunter. An employee of a state media outlet by day, at night he tries to debunk viral falsehoods using a Dell computer in his apartment in Shenyang, in China's north-east. He spoke to The Economist on the condition that his real name and his employer were not identified. Among the rumours Dianzizheng claims to have played a part in refuting are a story that organ harvesters were targeting subway stations for victims, and that 10,000 people had beaten up policemen in the southern province of Fujian. He also tries to track down the sources of rumours, though with little success. His enemies have at their disposal armies of zombie followers and fake re-tweets as well as marketing companies, which help draw attention to rumours until they are spread by a respected user with many real followers, such as a celebrity. Dianzizheng says real-name registration should help him and his fellow rumour-hunters, but accepts that it is unlikely to be decisive.

"We have a saying among us: you only need to move your lips to start a rumour, but you need to run until your legs are broken to refute one," he says, in a tone that is cheerful and tireless. He is motivated, he says, by the national interest. "I believe there is a huge risk to the country if rumours go unchecked." Perhaps so. Mr Lu, the historian, argues that the problem faced by the emperor Wang Mang in hunting down rumours 2,000 years ago was not the rumours themselves, but the truth that they reflected: a nervous public. In the age of weibo, it may be that the wisps of truth prove more problematic for authorities than the clouds of falsehood.

Table of Contents

The Anatomy of a Coup Rumour

By G.E., the Economist, Apr 5th 2012

AT NINE O'CLOCK in the morning on March 19th, financial journalist Li Delin tweeted on his account on Sina Weibo, a Chinese microblog, about unusually heavy traffic control on Beijing's central east-west thoroughfare, Chang'an Boulevard. Though the tweet has since been deleted (see Google cache here), he mentioned "military vehicles everywhere", "several plain-clothes at each intersection" and "iron barricades". Mr Li enjoys a good following on his microblog accounts (currently 23,000 on Sina Weibo, and more than 375,000 on the leading rival, Tencent Weibo), and the Sina tweet was forwarded, or retweeted, more than 200 times in less than four hours. The tweet on its own did not stir any trouble. But days later, friends said in their own remarks on microblogs, the journalist had been detained, possibly for that tweet. Mr Li, it seems, may have unwittingly helped spark the prairie fire of rumours of a coup attempt by powerful supporters of Bo Xilai, the ousted party secretary of Chongqing. Now the authorities have struck back against some of those spreading rumours (see related story).

Mr Li, a magazine journalist and the author of several books including "Goldman Conspiracy", is fond of fanciful and unsupported theories about Goldman Sachs' desire to undermine the Chinese state, in part through privatising state-owned enterprises—precisely the sort of theories that Mr Bo's Maoist partisans devour. Nevertheless, on March 19th Mr Li may have become implicated in a conspiracy theory that was not of his making. Although the details of his case are not entirely clear, his experience is an object lesson in the spread of rumours in the age of microblogs. It also shows precisely why the government is so nervous about rumours, which state media call the "malignant tumours" of the internet (see here in Chinese).

With Mr Li believed to be in custody (and unreachable; his mobile phone is switched off), it remains unclear what exactly he observed or heard about on the morning of March 19th, and whether any security measures might have had some official, innocuous purpose. Whatever the case, that evening, Mr Li's tweet took on a more ominous tone when it was cribbed and combined with other people's observations in new tweets. Just before 9pm, a microblog account billing itself as a news provider combined Mr Li's tweet with a blurry photograph of police vehicles on the street, purporting to be from that evening. Then a much more widely followed microblogger, businessman Shen Dongjun, took this stew of innuendo a big step further. Mr Shen, who has 1.9m followers on Sina Weibo, juxtaposed the photo and Mr Li's words with the tweet that evening of one of China's top microbloggers, billionaire real-estate developer Pan Shiyi (9.6m followers on Sina). Mr Pan had written: "Weibo is very weird tonight. Posts that contain certain words cannot be posted. [I] posted a tweet and saw the number of comments dropping, it scared me. Is there a ghost?"

Mr Shen's tweet at 9.10pm (viewable on Google cache here) was forwarded more than 2,000 times , and became part of the fodder for the wild rumours that night that there had been a coup attempt in Beijing (the tweet was removed the next evening, so it is unclear how many more times it was forwarded).

The confusion didn't end there. At 11.24pm, another microblogger, a self-proclaimed poet named Tang Yi, tweeted, "Gun fired! More big news for tomorrow! Mo Bai!" This was, Mr Tang explained several hours later, a reference to a radio programme he had written with a character named Mo Bai, utterly unrelated to anything happening in Beijing (he lives in southern China, far from the capital). But it had been forwarded more than 1,000 times by 3am, and some Chinese journalists wondered through the night whether there had been gunfire in Beijing.

By now Mr Li's comment about "military vehicles everywhere" had taken on much more conspiratorial meaning. The next day Mr Li, aghast, wrote a plaintive tweet that Mr Shen forwarded to his followers at 12.59pm on March 20th:

Mr Shen, I'm Li Delin. Now your post has made me very helpless. It was originally posted yesterday morning when there was traffic control, now everybody thinks it happened last night. The international media has made me unable to explain. [I] sincerely hope Mr Shen can clarify the rumours, thanks!

Unfortunately for Mr Li, that explanatory tweet seems only to have been forwarded (or retweeted) 24 times; similarly, another follow-up explanation of the "gun fired!" remark by Mr Tang, on March 22nd, was forwarded only four times. The feverish rumours of the coup spread much more widely than attempts to tamp them down.

Mr Li's apparent detention suggests he may be one of six people arrested for spreading the coup rumours—authorities have released only the surnames of the suspects, but his friends believe he is one of them. The authorities also ordered both Sina and Tencent to shut down comments on tweets for 72 hours from the morning of March 31st to the morning of April 3rd—a relative slap on the wrist, but a clear warning nonetheless.

In a narrow sense, this crackdown could have a chilling effect on the likes of journalists like Mr Li and perhaps even more for Mr Shen and Mr Pan—journalists and weibo celebrities whose tweets might be noticed. The Public Security Bureau summoned Mr Pan to give him a warning about his tweeting, according to a spokeswoman. Some others who tweeted or forwarded tweets about the rumours that night were also at least telephoned by police. (Mr Shen did not respond to a private message from The Economist on his Sina Weibo account). Authorities are also pushing Sina Weibo to enforce a requirement that microbloggers register with their real names; if they are successful, then in the future, rumour-mongers would be easily traced.

But the case of Mr Li demonstrates that quelling rumours is not just a question of getting tough. Gossip and rumour can get out of hand no matter the means of communication; that has been true since shortly after there were more than two humans on Earth, one suspects. Rumour-hunters, like the one we wrote about just before the coup rumours started, will always be outnumbered by their prey. Considering that, the release of Mr Li back out into the wild, as his friends are hopeful will happen, would seem a sensible resolution. Also sensible would be releasing trustworthy information in a timely manner. Governments in open societies are not nearly so concerned about the spread of internet rumours.

What is more interesting is what this spate of rumours and conspiracy theories might tell us about the times Chinese people are living in. As China's leaders prepare for their succession later this year, their nervousness about the spectating masses is all too palpable.

Table of Contents

The Inconvenient Astrologer of MI5

By Emma Garman, the Awl, April 11, 2012

In the summer of 1941, delegates at the American Federation of Scientific Astrologers' convention in Cleveland, Ohio, listened to a keynote address from an astrologer named Louis de Wohl. The bespectacled German-Hungarian—late thirties, rather corpulent, flamboyant in dress and confident in manner—told his rapt audience that Hitler was operating under advice from "the best astrologers in Germany," who had plotted out the course for Germany to attack the U.S. The invasion, it seemed, would occur sometime after the following spring, once Saturn and Uranus, the two "malefic" planets, had entered Gemini, America's ruling sign: "America," he warned, "has always been subject to grave events when Uranus transits Gemini." De Wohl's professional assessment, nonetheless, was that the stars portended eventual disaster for Hitler. "We can't predict a date for his defeat," he said, "but if the United States enters the war before next spring, he is doomed."

What no one realized was that de Wohl's lecture was pure propaganda from the British government, which was attempting to drag the Roosevelt administration into WWII by any means necessary. De Wohl, who was employed by SOE (Special Operations Executive, the wartime sabotage unit), had been dispatched with instructions to present himself as a renowned astrologer with no connections to Britain, and to undermine

America's belief in the invincibility of Hitler. As the spy novelist William Boyd put it in a 2008 radio interview: "At the time, there was a perception of American people, in the minds of the British Security Services, that they were more gullible than us Brits."

De Wohl's visit to Cleveland was part of a nationwide tour of talks and media conferences. He was interviewed by the New York Sun, which ran a story with the headline "Seer Sees Plot to Kill Hitler," detailing de Wohl's predictions that Hitler would be "done away within a year." In an interview with the New York Sunday News, headlined "Hitler's Stargazer Sees Heavenly Stop Light," de Wohl revealed that he'd obtained a letter written by Hitler's top astrologer, Karl Ernst Krafft, who confessed that in his opinion, Hitler wouldn't win the war and, indeed, would "suddenly disappear." The Los Angeles Times published a front-page report on de Wohl's forecasts, the most important being that unless America joined in the effort to defeat the Nazis, Germany would invade the country via Brazil.

De Wohl didn't shy away from making more immediate predictions, either. He announced that an important ally of Hitler, one who wasn't a German or a Nazi, would go insane within ten days. Lo and behold, the press soon reported that Admiral Georges Robert, the Vichy High Commissioner of the French West Indies, had lost his mind and could be heard shouting and screaming all night. Supernatural corroboration of de Wohl's prognostications came from far and wide: a Cairo newspaper published some prophesies from an Egyptian astrologer that eerily tallied with de Wohl's description of Hitler's downfall, as did the publicized visions of a Nigerian priest and the soothsaying of a Sierra Leonean stargazer.

Little wonder, then, that the public started to believe in de Wohl; they couldn't possibly have known that the press reports were planted by the British and the letter from Krafft was forged. It helped that American attitudes to astrology were less skeptical then, or so the ease with which de Wohl's predictions achieved credulous media coverage would suggest. He certainly talked the talk: Hitler's death was assured, he explained at a New York press conference, by Neptune entering his house of death at the same time as his progressed Ascendant conjuncting his natal Neptune, a set-up to be triggered by transiting Uranus. That Hitler would be alarmed by such confident prophesizing of his demise, since he supposedly believed in astrology, was a nice side-benefit.

De Wohl was in fact a practicing astrologer: in his 1937 memoir, I Follow My Stars, he describes the turning point of his life when, as a young novelist in Berlin, he meets a man whose ability to cast accurate horoscopes is so impressive that de Wohl himself is lured into the study of astrology. The relentlessly cheery and self-assured tone of this memoir, which portrays de Wohl as a plucky adventurer with prodigious creativity—he claims to have written his first novel at the age of 21, in a few weeks, while recovering from an illness—leaves the reader uncertain as to whether his "conversion" to astrology was genuine or merely a welcome opportunity for financial and social advancement. Either way, after leaving Germany in 1935, likely a necessity due to his being at least part Jewish, de Wohl settled in London, developed a reputation in powerful circles as a skilled fortuneteller, and was able to charge 30 guineas (more than $1000 in today's money) for a horoscope.

The nature of his clientele, which included foreign diplomats and military personnel, drew the attention of MI5, and senior intelligence officers decided it would be useful to recruit him. "As it is often of considerable interest to know who is consulting an astrologer and for what reason," wrote a Major Gilbert Lennox in a letter to the MI5 War Office, "and it is sometimes even more interesting to hear the advice which the stars give, I have made a private arrangement by which I get reported to me the names and details of Louis's clients."

De Wohl, meanwhile, was persuading the powers that be of the vital contribution he could make to the war effort: claiming that the dates of all Hitler's major coups were related to planetary aspects, he proposed that by reading the horoscopes of the Fürher and his henchmen, he could replicate whatever astrological advice the Third Reich was receiving, thus gaining much-needed insight into their confoundingly erratic military strategy. With this dubious brief, de Wohl was set up as a one man department: the "Psychological Research Bureau" occupied rooms at the Grosvenor House Hotel on Park Lane, where de Wohl prepared astrological reports on German military high-rankers.

According to Ellic Howe, who at the time was employed by PWE (the Political Warfare Executive, a clandestine propaganda unit reporting to the Foreign Office), none of the real spooks took de Wohl's reports seriously, but they realized that his astrological knowledge could be a worthwhile propaganda tool.

One scheme was the "revival" of a defunct German astrological magazine, Zenit, to be edited by de Wohl and distributed in Germany "by surreptitious means." Under the supervision of PWE chief Sefton Delmer, the magazine made predictions tailor-made to frighten the German forces. For example, a highly successfully German naval commander, Reinhard Suhren, was shown to have such a lucky horoscope that his subordinates would not face danger so long "as they are personally near him." Suhren, however, was soon promoted off his boat—a detail that British intelligence presumably knew in advance. Zenit's sixth and final issue also revealed

that SS leaders would soon betray Hitler. Lee Richards, in his book Black Art: British Clandestine Psychological Warfare Against the Third Reich, quotes Delmer on the experience of working with de Wohl:

> As I nervously put forward my views on what I rather hoped the stars might be foretelling, he frowned at me with terrifying ferocity, as though to reprove me for my infidel cynicism. Then he would grab up a handful of astrological charts from his Chippendale escritoire and make some rapid astral calculations. This done, he would turn once more to me, his frown now relaxed into a patronising smile. With the air of the master addressing a promising neophyte he would say in his guttural Berlin English: "How do you do it my friend? It is most extraordinary. There is something very much like you say. In the…" Then there would follow some, to me completely unintelligible, jargon about constellations, aspects, signs and so forth. But I had to keep the straightest of faces when making my suggestions. For my astrologer always insisted that he would under no circumstances be prepared to prostitute his sacred knowledge to purposes of subversion, much as he abhorred Hitler and what he stood for. It was simply a most fortunate coincidence that what I suggested so often fitted in with what the stars did indeed foretell.

Particularly useful was Zenit's accounting for the recent success of Allied naval forces in ambushing German U-boat submarines—in reality achieved thanks to MI5's cracking of the "Enigma" military code—by stressing the importance of heeding astrological factors if an "almost magical attraction for enemy cruisers and destroyers" is to be avoided.

Indeed, one of de Wohl's most valuable roles for British intelligence was as a front for information obtained by intercepting Enigma transmissions, which were used by the German High Command to convey orders. Once cryptanalysts at the famous Bletchley Park HQ had cracked the code, it was vital that no one knew about the enormously powerful tool at their disposal. So when passing on intelligence to field commanders, a nameable source was de Wohl's Psychological Research Bureau—and de Wohl, never the most modest of men, could brag about how his predictions were defeating the enemy.

It was de Wohl's obnoxious personality that, in the end, led to his ousting from the sphere of influence whose prestige he so enjoyed. He had even persuaded the colonel of a military intelligence department to confer upon him the rank of Army Captain; despite a promise of a total secrecy, he would "strut around" London decked out in military garb. An acquaintance has described seeing de Wohl in his "splendid officer's uniform" for the first time: "Louis was like a boy who had just received his Christmas presents. He stood up, he sat down, stood up again, walked around the room and looked into a large mirror in silent admiration." (De Wohl's love of costume extended to a penchant for cross-dressing, as his handlers gingerly noted.)

Apparently incapable of the discretion his position required, de Wohl was soon regarded in as a thorn in everyone's side—a note in his MI5 file, which was declassified in 2008, says: "He is much given to boasting, particularly about his connections with the War Office, Admiralty, etc. and would appear to an unsuitable type to be employed in any kind of secret activities."

Another concerned letter, dated May 1943, states: "I feel that there have now been so many indications that de Wohl is an indiscreet talker and a bumptious seeker after notoriety, that it would be insufficient merely to place him on the Unemployed List of the Army, and that he should be retired altogether."

The only problem was, exactly how could they quietly retire the man who had styled himself as Britain's State Seer? An aggrieved de Wohl was definitely not an appealing prospect, as had long been clear. When he returned from the States shortly after the bombing of Pearl Harbor—an event that, obviously, rendered his mission redundant—an MI5 officer wrote that de Wohl could easily "become a very dangerous enemy owing to the considerable influence which his charlatanism enables him to exert over the superstitious in high places." Three options to "dispose of him" were considered, including sending him away to live in a remote part of the country and restricting his movements. The other two options were ominously redacted.

In I Follow My Stars, de Wohl recounts visiting India in his early thirties and meeting a psychic yogi who predicts he will die at the age of 61. Actually, he didn't live quite that long, but he wasn't bumped off in his prime by MI5 either. Instead he gradually faded from prominence, converted to Catholicism and was rewarded for his services to the Allied cause with the British citizenship he dearly coveted, although he remained under MI5 surveillance until the end of 1945. After the war, de Wohl became a popular and prolific author of novels about the lives of saints, including Joan of Arc, St. Benedict and St. Francis of Assisi. His decade-long obsession with astrology was forgotten and, as it turns out, his entire career in the spy world was based on a falsehood anyway. While some of Hitler's henchmen, including Himmler, had some belief in astrology, it was officially banned in Nazi Germany and the man identified by de Wohl as Hitler's personal astrologer, Karl E. Krafft, would die in a concentration camp. "Hitler regarded astrology as nonsense," confirms Christopher Andrew, official historian of MI5, "but the belief that he really paid attention to horoscopes entered Whitehall."

It’s a historical misperception that endures to this day, thanks in no small part to the strange, unscrupulous and thoroughly mercurial Louis de Wohl.

Table of Contents

We Can Hear You Thugs

From Strategy Page, 22 April 2012

American and Israeli armed forces have been sharing data and ideas for decades. One recent success has been the use of Beechcraft King Air twin engine commercial aircraft for electronic warfare and reconnaissance against irregular forces (Taliban or Palestinian terrorists). The aircraft used is a commercial Beechcraft King Air, which can perform like a heavy (Predator or Reaper) UAV or an electronic warfare version crammed with vidcams, electronic sensors, jammers, and radios. This aircraft (Ceasar, for Communications Electronic Attack with Surveillance And Reconnaissance) can spend hours circling an Afghan battleground, keeping troops on the ground aware of enemy walkie-talkie and cell phone use, including location of these devices and translations of what is being discussed. The enemy is vaguely aware of what the militarized King Air (MC-12) can do but have no better way to communicate. Thus the few Caesar equipped aircraft sent to Afghanistan have proved very useful for the American and British troops that use them.

Military use of the King Air arose in the United States (where Beechcraft is located) began in the early 1970s when the U.S. Army adopted the King Air as the RC-12 and then used it for a wide variety of intelligence missions ever since. Israel was made aware of this technology and developed its own versions (the Tzufit).

But the Israelis had different needs and eventually developed a King Air equipped to deal with Palestinian terrorists who declared war on Israel in 2000. In the last decade Israel developed an intelligence collection version of the King Air that the U.S. only recently adopted as the MC-12 Ceasar. This new MC-12 version incorporates vidcams, as well all the electronic monitoring gear.

Two years ago the U.S. Air Force sent its first MC-12 "manned UAV replacement" to Afghanistan, and it proved successful. This despite the fact that it can only stay in action for seven hours (plus one to get to the target area) per sortie, which is half as long as a UAV can stay aloft. But more UAV capabilities (vidcams overhead for hours at a time) were needed in Afghanistan, and it didn't matter if the pilots are in the air or on the ground.

But the Americans knew, as the Israelis had discovered, that the King Airs were faster than UAVs, enabling them to get where they were needed more quickly, also the King Air carried more sensors than a UAV, which enabled it to be outfitted as a Ceasar aircraft. Moreover, having the equipment operators on board, along with a pilot and co-pilot available to just use their eyes on the target area, did make a difference over relying on operators elsewhere in Afghanistan, or somewhere else on the planet. That personal touch still makes a difference

It was four years ago that the first American MC-12 squadron was deployed to Iraq, where the twin engine aircraft was found to be durable and reliable and as useful as Israeli experience indicated. In six months those dozen aircraft flew over a thousand sorties in Iraq. That's about four sorties per week per aircraft. Most of the 37 MC-12s ordered have been sent to Afghanistan, where they have been worked hard and held up well to the heavy use. The arrival of these MC-12s was, in effect, the equivalent of increasing the Predator force by at least ten percent and adding a few more four engine electronic warfare aircraft (to eavesdrop on cell phones and walkies). Last year the air force ordered two more MC-12s.

The MC-12 pilots require a nine week training course, which includes simulator time and twelve flights in the actual aircraft. This converts the pilot of another aircraft type (fighter, tanker, transport) to one who can handle the MC-12. The two equipment operators can do all their training on a simulator. The MC-12 itself is a modified version of the much older RC-12 electronic reconnaissance aircraft.

The MC-12 provides the same service as a UAV (full motion video) in addition to electronic monitoring (radio, cell phone, etc.). The air force also converted some existing King Air 350s, as well as buying new ones, to obtain up to fifty MC-12s for duty as, in effect, a Predator UAV replacement. Most of these are in service now. These were a big help because UAVs cannot be manufactured fast enough to supply battlefield needs, so the manned MC-12s help fill the gap.

The King Air 350 is a 5.6 ton, twin engine aircraft. The MC-12 can stay in the air for up to eight hours per sortie. Not quite what the Predator can do (over 20 hours per sortie) but good enough to help meet the demand. The MC-12 has advantages over UAVs. It can carry over a ton of sensors, several times what a Predator can haul. The MC-12 can fly higher (11 kilometers/35,000 feet) and is faster (over 500 kilometers an hour, versus 215 for the Predator). The MC-12s cost about $20 million each, more than twice what a Predator goes for. The MC-12's crew consists of two pilots and two equipment operators. The Tzufits have a crew of

five. Some of the sensors are operated from the ground. The Tzufit's are earlier King Air models, and can't fly as high as the MC-12s. But Israel is a smaller place and the Tzufits are all the King Air that is needed. Moreover, the Tzufit crews fly along the Gaza and Leabanese border for years and have acquired a detailed knowledge of what is below. This makes their capabilities even greater than what the aircraft is capable of.

The King Air 350 (and earlier models) has long been used by the U.S. Army and Air Force as a light cargo and passenger transport (the C-12 Huron).

Table of Contents

US And China Engage In Cyber War Games

By Nick Hopkins, the Guardian, 16 April 2012

The US and China have been discreetly engaging in "war games" amid rising anger in Washington over the scale and audacity of Beijing-coordinated cyber attacks on western governments and big business, the Guardian has learned.

State department and Pentagon officials, along with their Chinese counterparts, were involved in two war games last year that were designed to help prevent a sudden military escalation between the sides if either felt they were being targeted. Another session is planned for May.

Though the exercises have given the US a chance to vent its frustration at what appears to be state-sponsored espionage and theft on an industrial scale, China has been belligerent.

"China has come to the conclusion that the power relationship has changed, and it has changed in a way that favours them," said Jim Lewis, a senior fellow and director at the Centre for Strategic and International Studies (CSIS) thinktank in Washington.

"The PLA [People's Liberation Army] is very hostile. They see the US as a target. They feel they have justification for their actions. They think the US is in decline."

The war games have been organised through the CSIS and a Beijing thinktank, the China Institute of Contemporary International Relations. This has allowed government officials, and those from the US intelligence agencies, to have contact in a less formal environment.

Known as "Track 1.5" diplomacy, it is the closest governments can get in conflict management without full-blown talks.

"We co-ordinate the war games with the state department and department of defence," said Lewis, who brokered the meetings, which took place in Beijing last June, and in Washington in December.

"The officials start out as observers and become participants … it is very much the same on the Chinese side. Because it is organised between two thinktanks they can speak more freely."

During the first exercise, both sides had to describe what they would do if they were attacked by a sophisticated computer virus, such as Stuxnet, which disabled centrifuges in Iran's nuclear programme. In the second, they had to describe their reaction if the attack was known to have been launched from the other side.

"The two war games have been quite amazing," said Lewis. "The first one went well, the second one not so well.

"The Chinese are very astute. They send knowledgeable people. We want to find ways to change their behaviour … [but] they can justify what they are doing. Their attitude is, they have experienced imperialism and they had a century of humiliation."

Lewis said the Chinese have a "sense that they have been treated unfairly".

"The Chinese have a deep distrust of the US. They are concerned about US military capabilities. They tend to think we have a grand strategy to preserve US hegemony and they see a direct challenge.

"The [Chinese officials] who favour co-operation are not as strong as the people who favour conflict."

The need for the meetings has been underlined in recent months as the US and the UK have tried to increase pressure on China, which they regard as chiefly responsible for the theft of billions of dollars of plans and intellectual property from defence manufacturers, government departments, and private companies at the heart of America's national infrastructure.

Analysts say this amounts to "preparation of the battlefield", and both the UK and the US have warned Beijing to expect retaliation if it continues.

In recent months, the US has made clear it is turning its military focus away from Europe towards the Pacific to protect American interests in the region.

"Of the countries actively involved in cyber espionage, China is the only one likely to be a military competitor to the US," Lewis said.

"US and Chinese forces are in close proximity and there are hostile incidents … The odds of miscalculation are high, so we are trying to get a clear understanding of each side's position."

Lewis believes the US is preparing to become more aggressive towards China, saying President Barack Obama has already tasked internal working groups in the White House to consider tougher sanctions.

Without naming China, a senior executive in the FBI told the Guardian the threats posed from cyber attacks were alarming.

"We know that the capabilities of foreign states are substantial and we know the type of information that they are targeting," said Shawn Henry, executive assistant director of the FBI's cyber unit.

"We have seen adversaries that have been in networks for many months or even years in some cases, undetected. They have essentially had free rein over those networks … They have complete ability to disrupt that network entirely."

Frank Cilluffo, who was George Bush's special assistant on homeland security, said the time had come to confront China.

"We need to talk about offensive capabilities to deter bad actors. You cannot expect companies to defend against foreign intelligence services. There are certain things we should do if someone is doing the cyber equivalent of intelligence preparation of the battlefield of our energy infrastructure.

"To me that's off grounds. That demands a response. What other incentive could there be to map our infrastructure in the event of a crisis?

"We have a stronger hand in conventional military and diplomatic means. We need to show them our cards. All instruments on the table. I think we do have to start talking active defence."

He said the US had to be proactive or, in time, people would start losing confidence in the integrity of the internet and computer systems.

"If I don't invest because I am afraid, if I don't use the web because I am afraid, if you lose trust and confidence in those systems, the bad guys have won. Checkmate."

The state department refused to speak about the war games, or say which officials took part.

A spokesman said: "The United States is committed to engaging countries to build a global environment in which all states recognise and adhere to norms of acceptable behaviour in cyberspace. We are engaging broadly with the Chinese government on cyber issues so that we can find common ground on these issues which have increasing importance in our bilateral relationship."

The Pentagon declined to comment or say which of its officials took part in the war games.

China has consistently denied being responsible for cyber attacks on the US and other western countries. It says it is also the victim of this kind of espionage.

The Chinese defence minister, Liang Guanglie, has said Beijing "stands firmly against all kinds of cyber crimes".

"It is hard to attribute the real source of attacks and we need to work together to make sure that this security problem won't be a problem," he said.

"Actually in China we also suffered quite a wide range [of], and frequent, cyber attacks. The Chinese government attaches importance also on cyber security and stands firmly against all kinds of cyber crimes. It is important for everyone to obey or follow laws and regulations in terms of cyber security."

The People's Daily, the Chinese newspaper that most reflects the views of China's ruling Communist party, said last year that linking China to internet hacking attacks was irresponsible.

"As the number of hacking attacks on prominent international businesses and organisations has grown this year, some western media have repeatedly depicted China as the villain behind the scenes."

Table of Contents