Information Operations Newsletter

US Army Space and Missile Defense Command
Army Forces Strategic Command
G39, Information Operations Division

The articles and information appearing herein are intended for educational and non-commercial purposes to promote discussion of research in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the original authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of the Army, or U.S. Army Strategic Command.

ARSTRAT IO Newsletter Online

Table of Contents

Vol. 13, no. 10 (September 2013)

The Fanciful World of Cyber Warfare

By Emily Crawford, the Young Witness, Sept. 3, 2013

The explosion was catastrophic. When the gas pipeline ruptured that day in Siberia in 1982, the detonation was so large that the North American Aerospace Defence Command headquarters, NORAD, initially thought it might have been a missile launch. Equivalent to three kilotonnes of TNT (or a small nuclear device), it was the largest non-nuclear explosion so far seen from space. Over 20 years later, a United States National Security Council staffer reported in his memoirs that the explosion was the result of an American sabotage operation. A Trojan horse computer virus had been embedded in the software that controlled the pressure and flow in the Siberian pipeline; in disrupting and manipulating the pressure, the virus placed stress on the pipes, ultimately leading to the massive explosion. It was, the staffer declared, the first-ever act of cyber warfare.

Except it wasn't.

When that National Security Council staffer - Thomas Reed - published his memoirs, journalists and experts set about testing his claims. They found the allegations were unverifiable. There were no media accounts that could confirm the explosion, even though accidents and explosions in the former Soviet Union were frequently reported in Western media at the time. Declassified internal Soviet accounts of computer sabotage during the height of the Cold War also failed to report any such activities. Even the former head of the KGB refuted Reed's report, suggesting he might have mistaken an explosion that happened earlier that year in the same region of Siberia. (In that incident, the thawing tundra had caused pipes to shift and fracture in the ground.) Even if such a lack of coverage could be chalked up to Soviet-era subterfuge and dissembling, technology experts claimed that such a ''logic bomb'' would have been almost impossible to hide in the basic software of 1982. All told, the preponderance of evidence combines to suggest that the so-called ''first cyber-war attack'' was a non-event.

This story of the Siberian pipeline ''attack that wasn't'' is among the examples Thomas Rid uses in Cyber War Will Not Take Place to demonstrate that cyber war, at least as it has come to be publicly discussed, has not, and will not, happen. Rid, a reader in war studies at King's College London, has emerged in the past few years as a sceptic in the increasingly hyperbolic public debate about cyber warfare and cyber security. And there has been plenty of hyperbole: a number of top US officials - including former Whitehouse ''cyber tsar'' Richard Clarke, former CIA director Leon Panetta, and the director of national intelligence for the Bush administration, Mike McConnell - have spoken of impending cyber-war disasters. Panetta has warned of a ''cyber Pearl Harbour'' and McConnell has prophesied a ''cyber equivalent of the World Trade Centre attack''. Calls for a ''cyber Geneva convention'' have abounded, and mass-media outlets have labelled computer viruses such as Stuxnet the ''Hiroshima of cyber war''.

Amid this commentary, Rid questions the prevailing doomsday analogies and comes to the firm conclusion that ''cyber war has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future''. He locates his assessment of the threat within an analysis of the nature of violence and warfare. Conflict, Rid says, must fulfil certain criteria in order to be classified as war. Drawing on Carl von Clausewitz's oft-quoted characterisation of war as ''an act of force to compel the enemy to do your will'', he argues that any war must involve violence of a political nature in order to compel another party to comply with a set of demands. Hostile acts in cyberspace, he argues, frequently fall short of von Clausewitz's three-part test: there is neither violence, nor political nexus, nor clear ends being sought. And so, he writes, ''the 'war' in 'cyber war' ultimately has more in common with the 'war' on obesity than World War II - it has more metaphorical than descriptive value''.

Labelling cyber attacks as cyber warfare is appealing - it's politically galvanising and emotive, and gives rhetorical force to what otherwise might be dismissed as troublemaking, a nuisance or ''mere'' criminality. Cyber warfare is a growth industry - most major military powers have dedicated cyber-security agencies reportedly developing offensive and defensive cyber-capabilities, preparing to fight in what's been termed the ''fifth domain of warfare'', alongside land, sea, air and space. NATO has its own Cooperative Cyber Defence Centre of Excellence in Estonia, which is tasked with developing cyber-defence capabilities for NATO governments and was integral to creating the recently released Tallinn Manual on the International Law Applicable to Cyber Warfare. The US has CYBERCOM - the US Cyber Command - covering cyber operations in the army, navy, air force and marines; the creation of CYBERCOM is reported to have spurred the creation of similar military agencies in Britain, China and South Korea. Indeed, even Australia has its own inter-agency Cyber Security Operations Centre, which includes personnel from the armed forces, ASIO and the federal police, and has recently announced the creation of a new cyber security centre.

As Rid argues throughout Cyber War Will Not Take Place, the rhetoric of warfare potentially distracts policymakers from the real and genuine threats in cyberspace - subversion, espionage and sabotage - which are closer to criminality than to warfare on the ''warfare spectrum''. Why this ''marriage'' of cyberspace and warfare is problematic is that the law of armed conflict does not, for the most part, concern itself with acts of espionage and sabotage. Provided such acts are carried out in compliance with the existing laws of armed conflict, espionage and sabotage are not considered violations of the laws of war. This is made explicit in the Tallinn manual's rule 66, which says ''cyber espionage and other forms of information-gathering directed at an adversary during an armed conflict do not violate the law of armed conflict''. In other words, continuing to view hostile acts in cyberspace through the prism of warfare opens up the potential for either ignoring the vast swathes of cyber hostilities that don't reach the requisite threshold for warfare or classifying all acts of cyber hostilities as warfare - neither of which is an ideal solution.

Cyber War Will Not Take Place was published before the Tallinn manual; as such, some of Rid's comments are already out of date. In discussing the policy debate surrounding cyber warfare, for instance, Rid says ''the debate and those trying to turn it into policy are getting ahead of themselves. Some fundamental questions on the use of force in cyberspace are still unanswered; worse, they are still unexplored.'' As of July 2013, this is no longer true; the Tallinn manual provides a detailed analysis of the law on the use of force and the law of armed conflict, and examines whether hostile cyber activities are regulated by that law and whether it needs to adapt to better regulate this kind of hostility. Oddly, the Tallinn manual - the result of three years of research and consultations with 20 experts drawn from government, the armed forces, academia and industry, already in train when Rid was writing his own work - is not mentioned in Rid's book.

This is not to say that the book has limited value. Rid provides a measured and well-researched analysis of cyber hostilities to date, and identifies where the real threat comes from: espionage, sabotage and subterfuge. Indeed, recent experience tends to support his contentions. The victims of the massive data theft from the Australian government, linked to Chinese hackers in May this year, were not only, or even primarily, military; rather, they were agencies such as ASIO, the Department of Foreign Affairs and Trade, the Department of the Prime Minister and Cabinet, the Reserve Bank and the Bureau of Statistics.

Rid stands as a useful voice among the Cassandras and Chicken Littles who warn of the impending cyber apocalypse. He bridges the divide between law and technology, and serves as the standard bearer for those hoping to lead the cyber-war debate out of what he calls the ''realm of myth and fairytale'' into rational, empirical discussion.

Table of Contents

Electronic Warfare: The Cat-And-Mouse Game Continues

By J.R. Wilson, Military Aerospace, 09 Sep 2013

Electronic warfare is one of the least known or understood areas of military combat. Far older than most, even in the military, realize, far more widespread and complex than most civilians imagine, it has become one of the most important offensive and defensive capabilities of any nation- or non-state organization, from drug cartels to terrorist groups.

EW's roots can be traced to the use of the telegraph as a means of military communications in the 1800s, which first led to blocking signals by cutting telegraph lines, then to intercepting-even spoofing-information and commands sent by wire. The arrival of wireless radio communications expanded the use of rudimentary EW and countermeasures, although the learning curve for those unaccustomed to such systems was steep.

An early example came during the 1905 Russo-Japanese War, when a Russian warship captain discovered a Japanese ship was transmitting the position of the Russian fleet to the Imperial Navy. His superiors denied his request to jam the signal, which no doubt played some role in Japan's overwhelming victory at the Battle of Tsushima Strait, where nearly 80 percent of the Russian Baltic Fleet was destroyed. As a result, Czar Nicholas II abandoned efforts to curtail Japanese expansion in East Asia, enabling Japan to emerge as a major world power.

The introduction of radar and more advanced communications capabilities made World War II the first major electronic warfare battlespace, with all major combatants constantly fielding new EW measures, countermeasures and counter-countermeasures. Much of what happened in the then nearly century-old-but still largely tactically and strategically new-form of combat remained classified even long after the war ended.

In 1967, Alfred Price, a 17-year veteran Royal Air Force EW officer turned historian, wrote Instruments of Darkness: The History of Electronic Warfare, in which he chronicled the rapid evolution of combat radio and radar during World War II and the counter-measures developed against them.

Technological battle

"[Those developments] led to a technological battle that neither the Axis nor the Allied powers could afford to lose," wrote Price, now a Fellow of the Royal Historical Society. "The result was a continual series of thrusts, parries, and counter-thrusts, as first one side then the other sought to wrest the initiative in the struggle to control the other."

As EW has grown in scope and importance in the military arsenal, secrecy has remained paramount. The vast majority of military users and U.S. Department of Defense (DOD) and contractor research and development labs decline comment on the state-of-the-art, much less new and evolving threats and technologies. Nonetheless, information does leak out, especially as DOD looks to a "Pacific pivot," where the U.S. has only two air bases west of Guam and the "tyranny of distance" creates new problems. That was highlighted in the "CNO's Navigation Plan 2014-2018," which Adm. Jonathan Greenert, Chief of Naval Operations, released last month.

"With our FY 2014-2018 budget submission, we will fully exploit cyberspace and the electromagnetic (EM) spectrum as a warfighting domain by fielding 20 additional E/A-18G Growler aircraft, developing the Next-Generation Jammer [NGJ] for airborne electronic warfare and delivering Surface Electronic Warfare Improvement Program [SEWIP] upgrades to improve the ability of DDGs [guided missile destroyers] to detect and defeat adversary radars and anti-ship missiles," he wrote. "[We also will] significantly expand the capacity of our offensive cyber capability and active defense by adding 976 cyber operators to stand up 40 cyber warfighting teams over the next three years."

Cyber warfare is a concept that arose with the use of computers and digital transmissions in the late 20th Century, but did not become a major (public) effort until the 21st. Today, every military service has a Cyber Command, as do all commands and units within the military. China, perhaps even more aggressive in developing military cyber capabilities, offensive and defensive, than the United States, has publicly declared its intention to be the world's top cyber superpower by mid-century.

Cyber warfare

"It is a huge capability that first requires you to get your mind around what it is, what it is not, and what it can be used for. The Air Force has done a good job of making it part of how we implement operations, giving commanders and planners a range of ops they did not have before. And if the enemy is complex, you need a complex toolbox," says Dan Faulkner, a former EF-111 EW jet officer who now serves as civilian chief of the Air Force Life Cycle Management Center's (AFLCMC) Materiel Integration Division. "I began with a very traditional EW mindset and I've had to get my head around cyber, which I now consider part of the planning and functions an EW warrior must have."

The emphasis given cyber in the same paragraph in which Greenert described the Navy's commitment to EW demonstrates how significant a part of electronic warfare it has become-and how it will continue to grow in importance as more and more military equipment, down to the individual warfighter level, and tactics, techniques, and procedures (TTPs) become reliant on computer chips and data transmissions and processing.

"What makes us smarter is knowing our enemies are smart and that we have to stay one step ahead of them," says Donn Rushing, project lead for the Navy's Maritime Unmanned Development and Operations. The cycle of EW systems development, threats, and counter-threats follows the same age-old pattern as armor/anti-armor-each new use of electronics leads to development of a way to intercept, jam, spoof, etc., which in turn leads to defensive counter-measures, then ways to counter the defenses, then a leap to new systems and so on. As computing power has become smaller, faster, cheaper, the cycle speed has far exceeded traditional military research and acquisition rates.

It also has expanded EW beyond its traditional weapons types-electromagnetic, directed-energy, and anti-radiation-across the full range of manned and unmanned air-, sea-, land- and space-based platforms. While the three major subdivisions of EW-Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (ES)-remain, what they entail is constantly evolving under what some are now calling Spectrum Warfare.

Beyond traditional limits

EA involves the use of the three primary weapons types to degrade, neutralize, or destroy enemy equipment, facilities, or personnel. That includes jamming or spoofing the enemy's own use of the electromagnetic spectrum and directed energy systems, including lasers, radio frequency (RF) weapons, and particle beams.

EP is the flip side, using defensive and counter-threat technologies to protect personnel, facilities, and equipment from all aspects of electronic attack.

ES, meanwhile, comprises actions tasked by an operational command- er to search for, intercept, identify, and pinpoint electromagnetic energy-weapons and common background-to determine what EW operations, offensive and defensive, are required to avoid and target enemy threats. Data gathered by ES operations also can be used for signals intelligence (SIG- INT), electronics intelligence (ELINT), and communications intelligence (COMINT).

As the level of civil use of the electromagnetic spectrum, from cell phones to Wi-Fi, ES has become increasingly important and difficult. "There is a tremendous growth in the number of sources emitting into the RF sector-whether EW or cell phones or wireless networks. The challenge we face with legacy and new systems is being able to discriminate within that environment what is a threat and take the appropriate countermeasure in a way the aircrew can effectively act upon it in a timely manner," says Col. Michael Kelly, chief of the EW & Avionics Division of AFLCMC's Program Executive Office-Agile Combat Support. "We need to ensure the legacy systems can do that, which we approach in a number of ways, hardware and software.

"But equipping legacy systems with the right software loads and so on for the environment in which the aircraft will be flown is the challenge. Everything radiates on its own portion of the spectrum, so any EW player is going to try to understand those, determine what characteristics can be used to determine what is a threat and what is not, then equip and program their system to the best of their ability to identify the threat and ignore other emitters. But as the environment becomes more congested, that becomes more challenging."

Precision-guided munitions

The past decade of war in Southwest Asia saw the development of more-and more accurate-precision-guided munitions (PGMs), from ship-, airplane-, and UAV-fired missiles to "smart" mortars. Those have reduced the number and destructive power needed to take out a specific target and the potential for collateral damage. That has been especially important in the SW Asian counter-insurgency (COIN) battle, where insurgents and terrorists have insulated themselves within or adjacent to mosques, schools, hospitals, and civilian homes and markets.

PGMs rely on precision GPS location and navigation, making efforts to jam or degrade GPS a top priority for the enemy. And, as adversaries acquire their own PGMs, for U.S. and allied forces, as well. Counter-measures include military-only signals that improve accuracy and enhance jam resistance.

At Patuxent River Naval Air Station, Md., the Naval Air Systems Command (NAVAIR) Facilities for Antenna and RCS Measurements (FARM) help test new GPS jamming and anti-jamming technologies. In July, the Navy conducted a series of tests on the use of miniaturized GPS protection devices to enable UAVs to operate despite enemy EW efforts.

A Small Antenna System (SAS) was mounted on an Aerostar UAV, then placed in a FARM room lined with signal-absorbent material and subjected to GPS jamming signals. Without its satellite guidance, a UAV would go off-course, possibly even crash, and be unable to relay critical intelligence back to a ground, sea, or airborne control station. That, in turn, would place U.S. and allied ships, aircraft, and submarines in jeopardy-a century-later version of the Battle of Tsushima Strait.

"If an enemy is trying to jam or interfere with the GPS frequency, this antenna allows us to track and acquire the true GPS satellites even in the midst of this jamming and interference," explains Eric Stevens, UAS Communications and Navigation lead for the Navy's Communications and GPS Navigation Program Office.

The tests were part of the Navy's effort to develop smaller and smaller GPS protection systems for UAVs, which have become an integral and crucial part of modern warfare, from intelligence, surveillance, and reconnaissance (ISR) to deep strike. Similar efforts seek to counter a growing variety of new offensive and defensive systems, including hostile digitally programmable radar and communications.

"The move to digital is something to which we are sensitive in developing our programs," says Faulkner, who also is co-chair of the Air Force EW Advisory Group's Technology Sub-group. "We have to move countermeasures with the technology, to understand and be responsive to it."

New technologies and upgrades

"We're developing new technologies to have a system organic to the aircraft, so you can reach destinations without relying on GPS," says Air Force Col. Keith Bearden, AFLCMC's director of program development and integration. "We realize the importance of GPS and so do our adversaries, so we are looking at how to deal with those. We're looking at multiple domains-GPS, improved organic systems, other elements in the environment; there are no bounds to where we are looking."

The same is true for potential adversaries-state and non-state-forcing the U.S. not only to identify what systems, threats, and countermeasures an enemy could employ today or may be developing for tomorrow,

then develop an effective counter to those, but also to make technology leaps to get ahead of everyone else. All those are further complicated by high technology becoming an increasingly available and affordable public commodity.

"There used to be a time when things were developed exclusively for the military; the problem now is other people have access to much of this," Bearden says. "You can go online and download the specs to build your own laser, even buy a kit; it's hard to control those things outside the military domain.

"Some of the threats are not very sophisticated, but effective, and we have to take that into consideration when developing the next generation," Bearden continues. "Precision navigation and timing are critical on just about everything we are developing and we incorporate the threat information we receive from intelligence into our new designs."

Non-traditional sources now have become an important part of the threat assessment provided by the intelligence community, Faulkner adds.

"We coined a term some years back-a confederated air defense system. You can even be a non-state actor, buying technology off the shelf, go on the black market to buy systems offered by some nations, and create your own air defense system. And that adds a level of complexity," he says. "Electronic warfare can be kinetic and non-kinetic. Non-kinetic tends to employ the EM spectrum and we run the gamut on electromagnetic, from classic EW jamming systems to cyberwar. We're not restricting ourselves along the electromagnetic, but balancing EM and kinetic. UAVs give us more of those capabilities, but we're also expanding our view of the EM spectrum to include cyber."

Some of those programs include:

1) Electronic Warfare Systems Integration Test Environment (EW SITE) upgrade-AAI is under contract from the Naval Air Warfare Center Weapons Division to provide one F/A-18 EW SITE test and measurement system and upgrade the Navy's existing EW SITE system by adding synthetic source instruments (SSIs).

2) Advanced Novel Spectrum Warfare Environment Research (ANSWER, nee Net-Enabled Electronic Warfare Technologies)-A planned AFRL-SD program to develop adaptive spectrum warfare technologies-electronic, optical, navigation, and cyber warfare-for use in future layered defensive systems and anti-access, anti-denial (A2/AD) scenarios.

3) Advanced Components for Electronic Warfare (ACE)-In July, AFRL awarded nine contracts for the ACE Phase 0 program to develop advanced and capable electronic and photonic components for tomorrow's EW systems.

4) The Boeing EA-18G Growler Airborne Electronic Attack (AEA) and P-8A Poseidon long-range anti-submarine warfare, anti-surface warfare and ISR aircraft.

5) Embarkable prototype shipboard EW system-An add-on advanced EW system being developed by ITT Exelis Electronic Systems and NRL to protect surface warships from a newly discovered, yet undisclosed, immediate threat to Navy fleet operations.

6) SEWIP-An evolutionary development, four-block upgrade program for the AN/SLQ-32 EW system to upgrade surface warship EW defenses against cruise missiles and other radar threats. Installed on aircraft carrier and surface and amphibious warships. Lockheed Martin and General Dynamics were awarded contracts in early 2013 for the first and second segments of the project.

7) Mixed-signal digital receivers-In February 2013, NRL's Tactical Electronic Warfare Division awarded a potential $16.7 million, three-year contract to Mercury Systems to supply advanced mixed signal digital receivers for prototype airborne and shipboard EW applications. The receivers will provide Navy EW researchers with ultra-fast tuning, high dynamic range, and extreme data processing.

8) Next Generation Jammer-A joint force wide-spectrum jammer, the NGJ could be applied to a wide range of missions; it also is intended to be the first in a family of open-architecture, software-driven, easily updated EW/EA systems able to conduct electronic attack from longer ranges than currently possible. Raytheon won the technology development contract in July, but a protest by BAE Systems has delayed start of the 22-month effort.

9) Army Electronic Warfare Planning and Management Tool (EWPMT) - On 3 July, the Army awarded a contract to Sotera Defense Solutions to develop planning software enabling warfighters to jam enemy communications, remotely controlled explosives, radar systems and other RF assets while safeguarding U.S. and allied RF systems.

Increasingly tight budgets are cutting sharply into new RDT&E and procurement, forcing the services to continue using legacy platforms and systems beyond their original end dates and retrofit technology to

upgrade them as much as possible. That also applies to EW platforms and systems, now a primary task for units such as the Air Force Life Cycle Management Center.

Although AFLCMC only stood up in 2012 with the consolidation of 12 Air Force Materiel Command centers to five, the Air Force Chief of Staff identified the need for a centralized effort in EW six years ago-including life cycle management.

"The EW & Avionics Division provides product support to fielded EW and avionics systems on U.S. Air Force and allied aircraft. We manage recurring operational flight software upgrades, sustaining engineering support, and occasionally modifying or acquiring new systems to go into fielded aircraft," Kelly explains. "We are not a basic research house and have relatively limited work in pre-acquisition technology development. Our focus is on supporting legacy systems and keeping them as viable as possible.

"We typically don't work directly with state-of-the-art technology; what we are bringing in terms of more modern technology is digital radio-frequency memory as an upgrade to some of our legacy systems. That basically expands their ability to assess what threats they are facing and the range of countermeasures that can be used. DRFM is not a new technology, but it is relatively new coming into the legacy and fielded systems."

Tight budgets

In the current economic environment, then, a major focus is on identifying "old" technologies that can be used in new ways and applications. One such effort is the ALQ-131A electronic attack pod upgrade-a self-protection jamming pod for F-16 and A-10 aircraft. Prime contractor Northrop Grumman is taking legacy ALQ-131 shells and incorporating high-power RF transmitters from ALQ-184 combat pods with a modern receiver and processing chain. Prototype testing is expected to end in 2014, with the new pods fielded in 2015.

"This will put what Northrop Grumman calls 'digital receiver exciter technology' in the pods," Kelly says. "I can't discuss specific threats it addresses, but it does put more modern technology and improved capability in the F-16s and A-10s, connecting to existing carriage, electrical, and control interfaces on the aircraft. We will buy pods according to the budget Air Combat Command can procure and those will be assigned in the fleet by ACC; the intent is to make pods available for ACC and the Air Guard and Reserve."

A similar use of existing technology to create a new EW capability is the ALR-69A radar warning receiver, which began fielding on Air Mobility Command C-130s in 2012, replacing their analog receivers with a digital system.

"That digital receiver gives us greater capability to detect and discriminate radar signals coming to the aircraft and identify them as threats to which the aircrew would need to respond," Kelly says.

Faulkner's office, on the other hand, is dealing with long-term capabilities, some of which may be applied to future legacy platforms, such as the F-35 or unmanned combat air vehicles (UCAVs).

Living without GPS

"We are developing weapons systems that can operate in GPS-degraded environments. I can't talk about it in detail, but there are a lot of methods, including fully optical, that are effective, but really expensive," Faulkner says. "We deal largely with systems that are 20 to 30 years away from IOC [initial operating capability], so we're looking at the full trade space-aircraft, UAVs, satellites, etc. But even today, things useful in EW don't necessarily have to have an 'E' in front of them; we now have options we did not have in the past. Putting a Hellfire missile on a UAV is a form of EW as it can just as easily target the kind of site an F-4 used to target with an anti-radiation missile.

"Today things move much more quickly, so you hope to stay at least a little bit ahead. And some of the basic principles that had been around forever no longer apply with advanced technologies. For example, if your jammer was more powerful than their signal, you could overwhelm it. But now your signal may be filtered out or their signal made so unique that brute force is no longer a guarantee. Power is still important, but with new technologies such as phased array, it is subject to debate," Faulkner adds.

For Bearden, the sometimes conflicting demands of new technologies, threats, and defenses with smaller budgets have made development planning the organic mission for program development and integration.

"It is a methodical process to develop a capability to a range of alternatives. We only have X amount of money to spend, so you have to make sure you spend it on the right thing" Bearden says. "We do a lot of the analysis and trade space work to bring the leadership alternatives on where to put our dollars-upgrade an existing system, develop a new system, just improve TTPs, or some combination. As dollars shrink, those become more important, not only with respect to systems that do exist, but also to those that might exist."

Table of Contents

Mysterious Actions of Chinese Satellites Have Experts Guessing

By Leonard David, Space.com, September 10, 2013

A set of three mysterious satellites has experts guessing about the Chinese space program's intentions. No one really knows what the Chinese are up to, and everything is speculation.

That appears to be the consensus of space experts tracking a set of Chinese spacecraft. Some have speculated that the Chinese are testing possible anti-satellite technology, while others have described the satellites as prosaic probes meant to sharpen the country's overall space skills.

Under debate are the orbital antics of several newcomers to space — the Chinese satellites Shiyan-7, Chuangxin-3 and Shijian-15 — which all launched into orbit together on July 20. Experts are also discussing the actions of China's elder spacecraft Shijian-7, which launched more than eight years ago. [Most Destructive Space Weapons Concepts]

One of the trio of new Chinese satellites, Shiyan-7 (SY-7, Experiment 7), has since made a sudden maneuver. That satellite had already finished a series of orbital alterations that put it close to one of the companion satellites with which it was launched, the Chuangxin-3 (CX-3).

"Suddenly, however, it made a surprise rendezvous with a completely different satellite, Shijian 7 (SJ-7, Practice 7), launched in 2005," noted Marcia Smith, a space policy analyst and founder and editor of SpacePolicyOnline.com.

'Arming' the heavens?

Soon after the July launch, it was known that one of the three satellites carried "a prototype manipulator arm to capture other satellites," a tool that might be "a predecessor of an arm destined to be aboard China's large space station, set for launch in 2020 or soon thereafter," wrote Bob Christy on zarya.info. (SpacePolicyOnline.com also reported the news.)

Christy could not confirm at the time which of the three satellites carried that arm.

When the three satellites were hurled skyward in July, the Chinese language press specifically discussed "space debris observation," "mechanical arm operations" and the testing of "space maintenance technologies," said Gregory Kulacki, a senior analyst and China project manager within the U.S.-based Union of Concerned Scientists' Global Security Program.

"This suggests one possible project for the mission is the experimental collection of space debris," Kulacki told SPACE.com.

The recent July 20 launch also resembles the lofting of the Changxin 2 and the Shiyan 3 satellites in November 2008, Kulacki said. Changxin 2 was an Earth observation microsatellite, while Shiyan 3 was an experimental spacecraft designed for space weather experiments, he said.

From benign to malign

The mystery surrounding the recent launches fits the Chinese pattern, said Dean Cheng, a research fellow on Chinese political and security affairs at the Heritage Foundation in Washington, D.C.

"Not sure why these are a surprise, other than that the Chinese don't tell us what they're going to do, so anything they do comes without a convenient press briefing," he said. [China's Shenzhou 10 Space Lab Mission in Pictures]

Close proximity maneuvers, like that between the two Chinese satellites, are consistent with a range of possibilities, from the benign (docking, refueling and repairs) to the malign (anti-satellite), Cheng told SPACE.com.

"But it is perhaps useful here to recall that the People's Republic of China remains intent upon establishing space dominance as part of their thinking about 'fighting and winning local wars under informationized conditions,'" Cheng said. And, even as the Chinese call for greater military-to-military contact with the United States, it's true "that they remain opaque, and that they pretty much refuse to engage the U.S. on military space issues."

That is, while China expands its space capabilities, the country is likely just as interested in military capabilities for their expanding array of space systems as it is in peaceful functions, Cheng said.

"Since space systems are largely dual use, it should not be surprising that there would be interest in the ability to maneuver satellites in close proximity … but neither should there be blithe assumptions that this is necessarily for solely peaceful ends," Cheng said.

Choice to make

An anti-satellite (ASAT) capability allows a country to render a satellite non-operational, Smith wrote.

"China conducted an ASAT test in 2007 when it launched a satellite interceptor against one of its own satellites. The test was successful in that it destroyed the satellite, but the resulting cloud of more than 3,000 pieces of space debris in a heavily used part of Earth orbit resulted in international condemnation, and spurred efforts to develop an internationally accepted code of conduct to ensure space sustainability," Smith said onSpacePolicyOnline.com.

But both China and the United States are experimenting with close-proximity maneuvers in space, said Michael Krepon, co-founder of the Washington, D.C.-based Stimson Center and director of its South Asia and Space Security programs. Both nations have demonstrated ASAT capabilities, Krepon told SPACE.com.

Information derived from actual or purported tests for ballistic missile defense, he said, can also be applied for ASAT purposes.

"Beijing and Washington have a choice to make, the same choice that Moscow and Washington faced during the Cold War," Krepon said.

"Major powers can ramp up a competition to damage satellites, or they can arrive at tacit agreements to dampen this competition," he said. "The United States and the Soviet Union chose wisely. China has yet to choose."

Table of Contents

Want to See China's Latest Top-Secret Military Site? Just Google It

By Dan Kedmey, Time World, Sept. 14, 2013

In the early days of the Cold War, the Soviet Union's May Day parade gave American spies an intelligence bonanza. As the latest Soviet fighter planes streaked overhead, U.S. diplomatic staff, scattered among the crowd, furiously snapped photos of the planes from miles below. With the advent of satellite technology, they no longer had to wait for the Soviet army's world premiere, as they could snap photos of secret military sites from space. The pictures astounded Lyndon Johnson, who learned that previous estimates of Soviet missile counts were hugely inflated. "We were building things that we didn't need to build," Johnson said at the time. "We were harboring fears that we didn't need to have."

Imagine, then, what his response might have been to the latest upheaval in intelligence gathering, whereby high-definition pictures of secret military installation turn up online, on obscure corners of the Web, for anyone to see. "The grainy photos that they were getting from those spy satellites were nothing compared to what you can get from Google Earth," says Peter Singer, director of the Center for 21st Century Security and Intelligence at the Brookings Institution. Singer and his co-researcher, Jeffrey Lin, recently wrote an analysis of China's latest covert project, its first homemade aircraft carrier, based on nothing but photos pulled from blogs. With a little Googling, anyone can find them.

Their analysis, published in Defense One, examines the ship's layout in startling detail. With a digital tape measure they sized up different parts of the ship, and with each measurement they reveal a new layer of meaning about its potential capabilities. An opening in the carrier's hangar, for example, measures from 6 m to 7 m in height, a tight squeeze for a J-15 fighter jet, but too narrow for bombers with heavier payloads.

If the analysis is correct, and they go to great lengths to list the unknowns as well as the knowns, then it provides a preview of how China could swing around its weight on the high seas. "It's not a match for U.S. force," Singer says of the carrier, "but it provides them with a signaling capability vs. their neighbors." China has recently engaged in naval jousting matches over tiny, disputed islands in the Pacific. Its neighbors might not defend their turf so vigorously if China one day parked a hulking aircraft carrier in disputed waters. "It's big deal for China vis-à-vis Vietnam, vis-à-vis Japan," Singer says.

The carrier pics are just a sampling of the intelligence that regularly turns up on the Internet. Singer ticked off a few recent examples: "New U.S. spy planes, unmanned systems — a.k.a drones — that weren't pushed under their hangars in time. Iranian missile sites. North Korean nuclear research plants.Strange patterns in China's hinterlands that people believe were used for a missile test site." The list goes on. These pictures can confound just about anyone's plans to keep things under wraps. And the intelligence cuts both ways for America's defense establishment. Singer says al-Qaeda militants used pictures of a helicopter off-loading materials at a military base in Afghanistan, along with coordinates from Google Earth, to plan an attack. The soldiers who uploaded the pictures had no idea they were providing the enemy with intelligence. They just thought it was a cool picture.

But perhaps the most fascinating point in this worldwide information dump is how it gets noticed in the first place. Jeffrey Lin is a 26-year-old graduate student of international science-and-technology policy at George Washington University. He developed an interest in military technology at the age of 14, when he commanded

tanks and jets in the computer game, People's General. Tired of waging fantasy battles across 20 different countries in Asia, he took to the Internet to learn about the reality of tanks, planes and modern weaponry. He became engrossed in two online discussion forums, China Defence Forum and SinoDefence.com, which linked up a community of military techies from all walks of life. Some identified themselves as retired vets and defense contractors, others, plain old enthusiasts. Lin would join these users in lengthy discussions of pictures that had surfaced from defense trade shows, official broadcasts or citizen journalists. The last group, in particular, has become an increasingly valuable resource, as China's smartphone penetration and broadband access have made it possible for just about anyone to snap a photo of strange pieces of defense equipment that pass within shutter range. Smartphone pictures of a fighter jet, wrapped under a tarp, strapped to a back of a truck barreling down the highway, now crop up on the forum.

At the same time, Lin developed an ability to parse the pictures for accuracy and meaning. He became a sort of digital-age Pocahontas, who could lead old-school intelligence experts through the unfamiliar terrain of crowdsourced pictures — fending off photoshopped pics, drawing hidden meanings out of seemingly insignificant details. He can look at the time stamp and the foliage of trees and conclude, "That's not in Shanghai or Xi'an simply because there's no snow on the ground." Gradually he narrows in on the location by process of elimination.

It was Lin who brought the pictures of China's aircraft carrier to Singer's attention. He spotted them in a post on China Defence Forum's blog. The fact that he may have been looking at the first images of China's first indigenous aircraft carrier didn't even surprise him. "Well, it's about time," he says. "We've been hearing on-and-off discussion about it for years."

Lin is just at the beginning of his career, but in a sign of how far these skills can take him, Singer points to one of the heavyweight champs of the open-source community. "Certainly one of the most important thinkers on U.S. Navy issues, is a guy who goes by the name Galrahn," Singer says. Galrahn is the user name of a man who has no connection to the Navy, and simply created a blog, Information Dissemination, which became the hub for arguing back and forth on Navy strategy. "Pull any Navy officer," Singer says, "and ask, 'Who are the top thinkers out there right now?' He would be listed in it."

No wonder, then, that the CIA set up a center for open-source intelligence in 2005, to distill the facts of online chatter from the rumors and drip-feed them into daily memos. This crowdsourced intelligence could never replace existing threat assessments, but it can strengthen them with supporting or opposing evidence. The Internet has redirected the flow of information from a few spies to a widening number of online users, and it's amazing how far this information can travel. Singer says he's seen it flow from the most obscure corners of the Internet, through niche media, to the mainstream media, before it at last reaches the desks of defense officials. "You'll see conversations that will start in one of these clusters and then end up in what's called the Early Bird," he says, referring to a memo of need-to-know news for top Pentagon officials.

Anyone reading this article right now may be a part of that information flow. The pictures of China's aircraft carrier have already been spotted by a bright, 26-year-old intern, who passed it on to a prominent think-tank expert, who wrote up an analysis in Defense One, which caught the attention of a curious journalist at TIME, who is now relaying the news to you, the reader, and who knows — it might even land in the inboxes of the military's top brass tomorrow morning, in the form of an Early Bird memo that's not so early after all.

Table of Contents

Redhack Announces Election Software as Its Next Target

By Nisan Su Aras, Hürriyet Daily News, 11 Sep 2013

With regard to the upcoming elections, Redhack will 'take the necessary steps to ensure a fair election,' a group representative told the Hürriyet Daily News. DHA photo

Redhack, the highly secretive hacker organization that has launched numerous cyber-attacks against official Turkish institutions, has identified the Computer Supported Central Voter Registry System (SEÇSİS), the official computer software program used in elections, as its next big target.

The group says it will "take the necessary steps to ensure a fair election," a Redhack representative told the Hürriyet Daily News.

"There are elections which will appear before us, and we have decided to take the necessary steps at least to have a fair election," the representative said.

"In the name of having a fair election and supervising this freak system called SEÇSİS, we have announced and will continue to announce who must be given the shoulder through social media, by giving support to IT experts and civil initiatives," he added.

However, Redhack stressed that it would not be intervening in SEÇSİS in terms of altering the election results, as this would only play into the government's hand. "We care more about supporting those who are experts on IT, digital information platforms and electronic infrastructure throughout the election process," the group added.

Redhack is composed of 12 core members, and decides on which online targets to attack based on its ideology, which it defines as "Marxist/Leninist."

"Our sole criterion is to select the institutions that cause events that hurt the public conscience; in other words, the institutions and capital groups that determine the oppressing attitude of the current system. Attaining the information, sharing this information and questioning the system by taking the public good into account are decisive in target selection," the representative explained to the HDN.

'Private Kalı did not leak Reyhanlı documents'

Redhack also denied any affiliation with Private Utku Kalı, who is currently being tried on terror charges for leaking intelligence documents on the Reyhanlı attack, in which 53 people were killed in Hatay province in late May. Redhack published these sensational whistle-blowing documents, indicating that a possible attack by al-Nusra was notified to the authorities in advance, but was not averted.

"We are not acquainted with Utku, he has never had any connection or contact with us," Redhack said, while arguing that he was declared a "scapegoat."

"Utku was rendered dependent on medical support due to heavy pressure, naked torture, and the inability to give a meaning [for the leaks] because of his innocence," it added.

Classified info flows after Gezi

Redhack increasingly came under the spotlight during the recent Gezi protests, and confirmed to the HDN that there had been a significant increase in information and documents sent to them after the Gezi incidents started.

"Without a doubt, almost every day tens of people get into contact saying they wish there was something they could do," Redhack said.

Redhack had previously not accepted information from outside the organization, but it had a change of heart after seeing the "manipulations of the media, the pressure on media laborers and disinformation tools."

It described its position during the Gezi protests as "information spreading." "We ensured that the messages of other components could spread to a wider mass. All this caused us to become quite prominent," it said.

The group has become more well known on an international level too, after Jeremy Hammond, a hacker/activist controversially imprisoned for publicizing the internal files of private spying agency Stratfor through Wikileaks, sent a letter to them saying "I like your attitude, brothers. I love you. Please keep on, sail strong."

Redhack was most notably involved in cyber-attacks against the websites of the Finance and Interior Ministries, the Religious Affairs Directorate and, most recently, that of the police department. It has also published e-mail exchanges between public and business figures, Reyhanlı intelligence files, and the telephone numbers of deputies and chiefs of police.

Table of Contents

Can the U.S. and China Get Along in Outer Space?

By Michael Krepon, Defense One, 17 Sep 2013

Space isn't just the final frontier. It's also a possible new frontier for warfare. The United States and China are ramping up capabilities to disable each other's satellites. A new Stimson Center collection of essays released on Tuesday, Anti-Satellite Weapons, Deterrence and Sino-American Space Relations, explores how developments in space will reflect and shape the mix of competition and cooperation between Washington and Beijing.

Satellites are force multipliers. The Pentagon already depends on them greatly; the People's Liberation Army (PLA) will depend increasingly on them in the future. Satellites back up and enable all U.S. military operations, everywhere, at all times. They help protect soldiers in harm's way. They provide intelligence, targeting support, damage assessments, communications, early warning, and weather forecasts that are essential for all military missions abroad.

These satellites are as vulnerable as they are invaluable. They cannot be armored like tanks and personnel carriers. A piece of space debris the size of a quarter can serve as an unintentional anti-satellite (ASAT) weapon. Its impact could create a mutating, pin-wheeling debris field that will kill other satellites in its path.

Intentional ASAT weapons also exist and cannot be dis-invented. Ballistic missiles, missile defense interceptors, lasers and jammers can be used to temporarily or permanently disable satellites. The PLA is improving and testing ASAT capabilities. The Pentagon is, too. An intensified competition in space weapons and the first-ever use of these capabilities in a deep crisis or a limited war between major powers could have catalytic consequences.

In 2007, the PLA carried out a “hit-to-kill” ASAT test against one of its aging weather satellites, causing the largest, human-made debris field in the history of the Space Age. The following year, the Pentagon demonstrated an agile, sea-based ASAT capability, blowing to smithereens a non-functioning intelligence satellite while entering the Earth’s atmosphere to avoid long-lasting debris consequences.

Beijing called its 2007 ASAT test an “experiment.” The Pentagon justified its 2008 test as necessary for public safety purposes, to prevent harm from the defunct satellite’s toxic fuel. The PLA has carried out subsequent “science experiments” and “ballistic missile defense tests.” There is considerable technical overlap between ASAT and ballistic missile defense applications. The Pentagon has carried out almost 60 missile defense tests in the last decade.

There have been far worse periods of military competition in space during the Cold War, the last being prompted by President Ronald Reagan’s Strategic Defense Initiative (SDI) in the 1983. Previous space war scares were handled with care because attacks on satellites could trigger a nuclear exchange. Washington and Moscow included protections of monitoring satellites in their nuclear arms agreements, and respected tacit “red lines” against highly provocative acts in space. The SDI led to deep cuts in nuclear forces instead of the weaponization of space.

While not as serious as space war scares during the Cold War, advances in U.S. and Chinese military space capabilities could foreshadow a worsening of bilateral relations. Or they could convince Beijing and Washington to engage in a constructive strategic dialogue. The Obama administration is willing, but Beijing’s new line-up of political leaders, like the one it replaced, still has cold feet.

Not talking about “the Bomb” was too unsettling during the Cold War. Vulnerability was inescapable. Deterrence needed parallel efforts at reassurance to keep the Cold War from becoming hot. Superpower nuclear arsenals were roughly comparable, opening the possibility for deals to be struck.

The U.S. and Chinese nuclear arsenals aren’t in any way comparable, so nuclear negotiations aren’t in the cards any time soon. But Beijing does have ambitious space plans. Its military will become dependent on vulnerable satellites, just like the United States.

Space capabilities, unlike nuclear arsenals, can be the door-opener for a strategic dialogue – if Beijing can shake its wariness of accords that require greater cooperation and transparency. In China, the PLA has out-sized influence on national security decision making – just as Soviet generals did when nuclear arms negotiations began.

The vulnerability of humankind to nuclear exchanges has always been obvious. The vulnerability of satellites – which could have profound consequences for humankind – is not glaringly obvious. Nor is there widespread public consciousness of how warfare in space could have catalytic consequences on Earth.

Beijing, along with Moscow, has proposed a gambit reminiscent of the early Cold War years: a pie-in-the-sky, unverifiable and unenforceable treaty that would ban the threat or use of force in space – but not military developments that would allow improvements in space war-fighting. The Obama administration has endorsed a European Union-led initiative to establish a code of conduct for responsible space-faring nations.

An ambitious space treaty is inconceivable, but an executive agreement setting rules of the road for space could have strategic significance. At present, the Obama administration is too distracted and Beijing is too wary to seize this opportunity.

Table of Contents

Meet Hidden Lynx: The Most Elite Hacker Crew You’ve Never Heard Of

By Dan Goodin, Ars Technica, Sept 17 2013

A hacking team with unusual skill and persistence has penetrated more than 100 organizations around the world, including US defense contractors, investment banks, and security companies whose sole purpose is to defend against such attacks, according to a detailed report.

One of the best known exploits of the so-called Hidden Lynx group was the devastating compromise of security firm Bit9 in 2012. The Waltham, Massachusetts, company provides an "application whitelisting"

service that allows customers to run only a small set of approved software on their PCs and networks. By hacking into the company's servers and stealing the private cryptographic keys Bit9 used to digitally sign legitimate apps, the intruders were able to infect more valuable targets inside military contracting firms who used the service.

Until now, little has been known about the group responsible for the Bit9 attack. Now, a detailed report released by security firm Symantec reveals it was a highly organized gang of hackers that has breached some 100 companies and government organizations around the world since 2009. They're dubbed the Hidden Lynx gang, based on a text string found on one of the command and control (C&C) servers they use to communicate with infected machines inside the organizations they compromise.

"From the evidence seen, it's clear that Hidden Lynx belongs to a professional organization," the report stated. It continued:

> They operate in a highly efficient manner. They can attack on multiple fronts. They use the latest techniques, have access to a diverse set of exploits, and have highly customized tools to compromise target networks. Their attacks, carried out with such precision on a regular basis over long periods of time, would require a well-resourced and sizeable organization. They possess expertise in many areas, with teams of highly skilled individuals who can adapt rapidly to the changing landscape. This team could easily consist of 50-100 individuals. This level of resources would be needed to build these Trojans, maintain infection and C&C infrastructure, and pursue confidential information on multiple networks. They are highly skilled and experienced campaigners in pursuit of information of value to both commercial and governmental organizations.

The Bit9 intrusion underscores the resourcefulness and persistence of the group. As thorough as that attack was, the hack was a mere detour taken on a longer path in a much more serious campaign. Dubbed VOHO, that campaign targeted US defense contractors. As it turned out, many of the VOHO targets used Bit9's application whitelisting service to prevent malware infections.

"When the Hidden Lynx attackers' progress was blocked by this obstacle, they reconsidered their options and found that the best way around the protection was to compromise the heart of the protection system itself and subvert it for their own purpose," Symantec analysts wrote in a separate Web post. "This is exactly what they did when they diverted their attention to Bit9 and breached their systems. Once breached, the attackers quickly found their way into the file signing infrastructure that was the foundation of the Bit9 protection model. They then used this system to sign a number of malware files and then these files were used in turn to compromise the true intended targets."

The report said the group is divided into two teams that use separate malware tools and sometimes work independently of each other. Team Moudoor, named for the trojan they use, takes a large-scale approach that broadly penetrates organizations in the financial industry, local and federal government organizations, and organizations related to healthcare, education, and law. Team Naid, by contrast, is more of a special operations squad that keeps a low profile so it can save its resources for the highest-profile targets in the defense industrial base.

The group pioneered so-called watering hole attacks, which infect a site with malware in the hopes of compromising the high-value targets known to frequent it. Members wield advanced, zero-day attacks that exploit security vulnerabilities in Oracle's Java, Microsoft's Internet Explorer, and other widely used software frameworks or applications. The report said their tactics and exploits are far more advanced than those of the Comment Crew, a China-affiliated hacking crew that researchers from security firm Mandiant said has siphoned terabytes of sensitive data from 141 organizations over the past seven years. Hidden Lynx also wielded one of the trojans that was used by the group that breached Google and at least 34 other companies in 2010.

"Given the breadth and number of targets and regions involved, we infer that this group is most likely a professional hacker-for-hire operation that is contracted by clients to provide information," Symantec researchers wrote. "They steal on demand, whatever their clients are interested in, hence the wide variety and range of targets."

Table of Contents

Hacking U.S. Secrets, China Pushes for Drones

By Edward Wong, New York Times, September 20, 2013

BEIJING — For almost two years, hackers based in Shanghai went after one foreign defense contractor after another, at least 20 in all. Their target, according to an American cybersecurity company that monitored the attacks, was the technology behind the United States' clear lead in military drones.

"I believe this is the largest campaign we've seen that has been focused on drone technology," said Darien Kindlund, manager of threat intelligence at the company, FireEye, based in California. "It seems to align pretty well with the focus of the Chinese government to build up their own drone technology capabilities."

The hacking operation, conducted by a group called "Comment Crew," was one of the most recent signs of the ambitions of China's drone development program. The government and military are striving to put China at the forefront of drone manufacturing, for their own use and for export, and have made an all-out push to gather domestic and international technology to support the program.

Foreign Ministry officials have said China does not sanction hacking, and is itself a victim, but another American cybersecurity company has tracked members of Comment Crew to a building of the People's Liberation Army outside Shanghai.

China is now dispatching its own drones into potential combat arenas. Every major arms manufacturer in China has a research center devoted to drones, according to Chinese and foreign military analysts. Those companies have shown off dozens of models to potential foreign buyers at international air shows.

Chinese officials this month sent a drone near disputed islands administered by Japan; debated using a weaponized drone last year to kill a criminal suspect in Myanmar; and sold homemade drones resembling the Predator, an American model, to other countries for less than a million dollars each. Meanwhile, online photographs reveal a stealth combat drone, the Lijian, or Stealth Sword, in a runway test in May.

Military analysts say China has long tried to replicate foreign drone designs. Some Chinese drones appearing at recent air shows have closely resembled foreign ones. Ian M. Easton, a military analyst at the Project 2049 Institute in Virginia, said cyberespionage was one tool in an extensive effort over years to purchase or develop drones domestically using all available technology, foreign and domestic.

Chinese engineers and officials have done reverse engineering, studied open source material and debriefed American drone experts who attend conferences and other meetings in China. "This can save them years of design work and mistakes," Mr. Easton said.

The Chinese military has not released statistics on the size of its drone fleet, but a Taiwan Defense Ministry report said that as of mid-2011, the Chinese Air Force alone had more than 280 drone units, and analysts say the other branches have thousands, which means China's fleet count is second only to the 7,000 or so of the United States. "The military significance of China's move into unmanned systems is alarming," said a 2012 report by the Defense Science Board, a Pentagon advisory committee.

China's domestic security apparatus, whose $124 billion official budget this year is larger than that of the military, is also keenly interested in drones, which raises questions about the potential use of drones for surveillance and possibly even attacks inside China, including in restive areas of Xinjiang and Tibet. Drone technology conferences here are attended by both military and domestic security officials. An international conference on nonmilitary drones is scheduled to take place in Beijing from Sept. 25 to 28.

A signal moment in China's drone use came on Sept. 9, when the navy sent a surveillance drone near the disputed Diaoyu Islands, which Japan administers and calls the Senkakus. Japanese interceptor jets scrambled to confront it. This was the first time China had ever deployed a drone over the East China Sea. The Chinese Defense Ministry said "regular drills" had taken place "at relevant areas in the East China Sea, which conform to relevant international laws and practices."

The drone appeared to be a BZK-005, a long-range aircraft used by the Chinese Navy that made its public debut in 2006 at China's air show in Zhuhai, said an American official.

Mr. Easton said deploying the drone near disputed waters and islands "was very much a first" for China and had caught Japanese officials off guard.

"I think this is really just the beginning of a much broader trend we're going to see — for China to increase its ability to monitor the East China Sea and the Western Pacific, beyond the Philippines, and to increase the operational envelope of their strike capabilities," he said.

The Chinese military, with its constant focus on potential war over Taiwan and an eye on China's growing territorial disputes, is at the vanguard of preparing drones for use in maritime situations. That is unlike the

United States, which has used drones to hunt and kill suspected terrorists and guerrilla fighters, mostly in Pakistan and Afghanistan.

American drones “are not designed to enter into contested or denied air space,” Mr. Easton said. “So they would be unable to fight in any conflict with China.”

China, on the other hand, is building drones, also called unmanned aerial vehicles, precisely to operate in contested spaces. “It’s a very useful instrument for safeguarding maritime sovereignty,” said Xu Guangyu, a retired major general and director of the China Arms Control and Disarmament Association. “China will gradually step up its use of U.A.V.’s in this area.”

Chinese strategists have discussed using drones in attack situations if war with the United States were to break out in the Pacific, according to the Project 2049 report. Citing Chinese military technical material, the report said the People’s Liberation Army’s “operational thinkers and scientists envision attacking U.S. aircraft-carrier battle groups with swarms of multimission U.A.V.’s in the event of conflict.”

University research centers are at the core of China’s drone program. The oldest research and production center for drones is the Northwestern Polytechnical University in Xi’an, where design work began in 1958. The ASN Technology Group, linked to the school, said on its Web site that it produces 90 percent of Chinese drones.

At the program’s start, China reverse-engineered drones it had acquired from the Soviet Union in the 1950s. It also got its hands on American drones that crashed in Vietnam in the 1960s and in China while monitoring China’s nuclear weapons program. China bought 100 Harpy armed drones from Israel in the 1990s — its only significant purchase of foreign-made drones — and the Pentagon later pressured Israel not to upgrade those drones for China.

In recent years, China has continued to acquire foreign drone technology and is especially focused on studying American models. “American U.A.V. technology is very sophisticated,” Mr. Xu said. “We can only envy their technology. Right now, we’re learning from them.”

For the Obama administration and American business executives, no method of Chinese technology acquisition is more worrisome than cyberespionage. An American official confirmed that drone technology had been stolen by hackers.

FireEye, the cybersecurity company in California, called the drone theft campaign Operation Beebus, traced back to a command-and-control node at bee.businessconsults.net. Cybersecurity experts say that general address and tools linked to it are associated with the Comment Crew, the Chinese hacker unit that Mandiant, another cybersecurity company, discussed in a report in February. Mandiant said the group was part of Unit 61398 of the People’s Liberation Army, based in Shanghai.

Though the initial victims in Operation Beebus were large defense contractors, the hackers began to pick out companies that specialized in drone technology, said Mr. Kindlund, FireEye’s threat intelligence manager. They then alternated between large companies that made a wide range of military technology and boutique firms that focused on drones.

In China, it is not just the military that is looking at uses for drones. In February, Liu Yuejin, the director of the antidrugs bureau in the Ministry of Public Security, which is responsible for domestic security, told Global Times, a state-run newspaper, that the ministry had considered using a drone armed with 44 pounds of explosives to kill a Burmese man in northern Myanmar suspected of ordering the murders of 13 Chinese sailors on the Mekong River. In the end, the idea was shelved because senior Chinese officials wanted the suspect, Naw Kham, captured alive.

Chinese drones are increasingly appearing in the arsenals of other nations. The Chinese version of the Predator, the Wing Loong, or Pterodactyl, was first exported in 2011, according to People’s Daily. At the Paris Air Show in June, the president of a Chinese aeronautics company told Global Times that the drone could carry two laser-guided missiles and was the equal of the Predator in endurance and flight range, but was much cheaper.

Table of Contents

Metadata May Not Catch Many Terrorists, but It's Great at Busting Journalists' Sources

By Shane Harris, Foreign Policy, September 24, 2013

The National Security Agency says that the telephone metadata it collects on every American is essential for finding terrorists. And that's debatable. But this we know for sure: Metadata is very useful for tracking journalists and discovering their sources.

On Monday, a former FBI agent and bomb technician pleaded guilty to leaking classified information to the Associated Press about a successful CIA operation in Yemen. As it turns out, phone metadata was the key to finding him.

The prosecution of the former agent, Donald Sachtleben, brings the number of leaks prosecutions under the Obama administration to eight, nearly three times the number prosecuted under all previous administrations. What's driving this record-breaking prosecution of leakers? Is it that this president especially despises loose talk with reporters and the time-worn culture of Washington backstabbing that they represent?

Not likely. The real reason the government is going after leakers is because it can. Investigators today have greater access to phone records and e-mails than they did before Obama took office, allowing them to follow digital data trails straight to the source.

After the AP published its big scoop on the Yemen operation, on May 7, 2012, FBI investigators started looking for the source of the story. They interviewed more than 550 officials, but they came up short.

So, in a highly controversial move, investigators secretly obtained a subpoena for phone records of AP reporters and editors. The records, which included the metadata of who had called whom, and how long the call lasted, covered a period in April and May of 2012. That was right around the time that the AP was reporting the Yemen story.

Once investigators looked at that phone metadata, they got their big break in the case.

"Sachtleben was identified as a suspect ... only after toll records for phone numbers related to the reporter were obtained through a subpoena and compared to other evidence collected during the leak investigation," the Justice Department said yesterday in a statement. "This allowed investigators to obtain a search warrant authorizing a more exhaustive search of Sachtleben's cellphone, computer and other electronic media..."

The reporter is not named in the court documents, but two of the AP's best investigative journalists, Adam Goldman and Matt Apuzzo, wrote the Yemen story.

The phone metadata wasn't just the key to Satchleben. It sped up the investigation dramatically. The FBI had conducted 550 fruitless interviews, and with one scan of a reporter's phone record, they had their man. It's no wonder that the Obama administration is going after leakers so often. Metadata is the closest thing to a smoking gun that they're likely to have, absent a wiretap or a copy of an email in which the source is clearly seen giving a reporter classified information.

The subpoena of the AP's records was roundly criticized by press groups. The Justice Department didn't tell AP about the subpoena in advance, as is customary in these cases. And the department didn't reveal until May 2013, a year after the story ran, that investigators had been combing through journalists' phone logs.

The AP called the secret subpoena a "massive and unprecedented intrusion" into the news-gathering process. And it may have resulted in a backlash. Sources close to the Justice Department have said recently that investigators are unlikely to aggressively go after a leaker via a reporter's phone records again because of the controversy over the AP case. They've also been chastened in another leaks investigation, in which a Fox News reporter was named as a potential co-conspirator because he asked his source for information, a move that drew similar howls from press advocates.

Of course, the FBI doesn't just look at reporters' phone records. They can examine government employees' work phones and email accounts without a warrant. The FBI also had a stroke of unexpected luck in the Sachtleben case, because the government had already seized his cell phone and computer as part of a child pornography investigation. When the FBI found the link to the AP reporter in the phone records, they scanned Sachtleben's devices. On his phone, they discovered text messages and records of calls between Sachtleben and an AP reporter -- again, he's not named in court documents -- about a notorious Yemeni bomb maker. On May 2, Sachtleben visited a lab where U.S. technicians were examining a new underwear device that the bombmaker had built, and that had been captured by the CIA before it could be used, the documents say. This was the germ of the AP's story, which ran five days later.

But the FBI would not have been tipped to Sachtleben as the AP's source in the first place absent that link from the reporter's phone records. If you're looking for a case study in the power of metadata, you've found it.

Table of Contents

Fooled by Certainty

By Michael C. Sevcik, Small Wars Journal, June 28, 2013

"It's not what you don't know that gets you into trouble. It's what you know for sure that just ain't so." Mark Twain [1]

Certainty is pervasive in our world. Just look at the opinion section in the local newspaper or open some of those outrageous email messages. Water boarding is torture – PERIOD! The Tea Party: brainwashed idiots, not patriots. Occupy Wall Street protesters are morons. These tax and spend democrats with Obamacare will bankrupt the nation. Abortion is murder of an unborn child. Pro choice is a woman's right. Global warming is an Inconvenient Truth or a bunch of hogwash. The world was created in six days and on the seventh day, God rested. It took over four billion years for life to evolve.

Certainty is sometimes funny. A UFO was recovered at Roswell, NM in 1947 and the USAF has alien bodies hidden at Wright Patterson, AFB. John F. Kennedy's assassination was planned by the CIA and it is common knowledge that Princess Diana was murdered by the Royal Family because she made the queen look fat.

Importantly, certainty is dangerous! Certainty in his political views for a new Arian race drove Adolph Hitler resulting in a world at war, millions dead and the unthinkable horror of Jewish concentration camps. Bolshevik revolutionaries encouraged by Joseph Stalin's certainty killed an estimated 20 million with over half starved to death in the Soviet Gulag Archipelago. The 20th century title holder for murder however, was Mao Tse-Tung -- his certainty in the cultural revolution resulted in an estimated 35 – 50 million deaths mostly from starvation during China's 'Great Leap Forward.' More recently, certainty persuaded 19 young Muslims from Saudi Arabia to skyjack US airliners and fly them into the Pentagon and World Trade Center complex. The result is well known, almost 3000 Americans dead on 9-11 resulting in the global war on terror which many readers have been fighting since. In November 2009, certainty in the mind of Major Nidal Malik Hasan motivated him to shoot and kill 13 fellow Soldiers and wound 29 others at Fort Hood, Texas.

Certainty may creep into the mind of an Army commander serving in Afghanistan. Staff principals assure him that there is absolutely no way there are friendly forces in the vicinity of an airstrike. Besides, the strike is planned for inside Afghan territory and we have coordinated with Pakistani forces. Result – 24 allies, Pakistani Soldiers dead, a military disaster and a political mess.[2] Closer to home, certainty that the world cannot go on without his sweetheart reasons a young 19 year old Soldier at Fort Hood tonight—result yet another tragic suicide.

Background

The thesis of this paper is as old as the human race; it's about the brain but more specifically about a problem that is literally and figuratively, inside the mind. It's about the mind which controls every aspect of human behavior and activity. It's an important topic for the military professional because through thinking, decision-making and judgment, the human mind dominates all aspects of land, sea, air, space and cyber operations.

Danish philosopher Kierkegaard noted almost 200 years ago, "There are only two ways to be fooled. One is to believe what isn't true; the other is to refuse to believe what is true." An important goal of behavioral decision-making research is to improve our understanding of the processes underlying judgments and decision-making. The logic is that a better understanding of human judgment will lead to better decisions and lessen the chance of being fooled. "In what is now considered classic work, fundamental biases in judgment and choice, and systematic deviations from rational behavior are consistent and universal. Recent behavioral decision-making research has shifted towards investigating the underlying cognitive processes that lead to these fundamental biases. " [3] One important cognitive process and a fundamental bias in the human race is the topic of this paper: your feeling of "certainty." While there are myriad human biases, most of us take it on faith that our personal feeling of certainty is accurate and true. Be careful, your own feeling of certainty is perhaps the mother of all bias. The hypothesis is straightforward -- the feeling of certainty you possess is often nothing more than a deceptive bias and as Kierkegaard and Mark Twain mentioned above, a problem.

Certainty originates primarily from emotion and to a lesser degree, from the senses. Judgment, reason and thinking also lead to the feeling of certainty but they contribute much less than emotion and your personal sense of reality experienced through the senses. To explain how the mind, through emotion and physical senses give us the feeling of certainty, it's important to point out several biological underpinnings of the human brain. The physiology of minute chemical reactions and the vast electrical firing of neurons in the

brain comprise the mysterious and complex neural network. Understanding the neural network is impossible but a partial understanding is important in order to think and learn. Thinking and learning leads all of us to the feeling of certainty.

The feeling of certainty rather than "certainty" is important because 'how you know what you know' has a profound impact on human judgment and decision-making. Moreover, the degree of certainty we hold in our mind, colors our perception of the operational environment, our beliefs and our sense of reality. Our religious, political, moral beliefs are demonstrably driven by emotions and mostly devoid of logic or reason.[4] Many people are dogmatically certain of their moral, religious or political views. This feeling of knowing (absolute certainty) is not just an ordinary human bias -- it is in fact how we are emotionally, psychologically and pathologically wired.

The thesis of this paper originates from Robert A. Burton, M.D. and is illustrated in his book, "On Being Certain." A medical doctor and neurosurgeon--the premise:

> "You cannot logically or reasonably determine between your thoughts that are correct or incorrect. Certainty and similar states of 'knowing what we know' are sensations that feel like thoughts, but arise out of the involuntary brain mechanisms that function independently of reason. The feeling of knowing (certainty) is very similar to other emotions such as love, anger or hate but importantly – the feeling of knowing in itself, functions independently from reason. This feeling is not a conscious choice or thought process." [5]

Dr. Robert A. Burton's important work sheds light on the science behind the feeling of knowing. With years of medical and scientific experience studying the brain, Burton demonstrates how we perceive our external world through our physical senses but the internal world of our mind is manifest through "feelings" such as familiar or strange, correct or incorrect, certain or uncertain. Cognitive science has raised the possibility that "…the very building blocks of thought might be subject to involuntary, even genetic influences that make each of us 'private islands' of perception and thinking."[6] Starting with results from neuropsychology and psychology Dr. Burton demonstrates that the degree of certainty people attach to thinking originates before conscious thought. This "certainty" or feeling of knowing is difficult to change once we experience it even in the light of overwhelming empirical evidence. In fact, most people often admit the truth of the evidence, but still cling to their inconsistent yet certain beliefs.

For example:

"In 1986, after the space shuttle Challenger disaster, a psychology professor, Ulric Neisser had his students write precisely where they'd been when they heard about the explosion. Two-and-a-half years later, he asked them to recall the same information. The students expressed high levels of confidence that their memories were right. While fewer than one in ten got the details right, almost all were certain that their memories were accurate and in fact, many couldn't be dissuaded even after seeing their original notes."[7]

The feeling of knowing described in the example above is partially explained by the role of emotions originating from the limbic system deep inside the human brain. The limbic system includes the oldest regions of the cortex and sub-cortex, in addition to being the source of emotion contains the brain's primary reward system. Neurology and science have long known that in addition to involuntary genetic influences, emotion plays a pivotal role in our views about morality.[8] The role of emotion is important in the discussion of the feeling of certainty because, "we perceive or external world through primary senses such as sight, sound, smell however, we perceive our internal world through emotional feelings such as familiar or strange, real or unreal, correct or incorrect, certainly true or false."[9] Importantly, from Dr. Burton's work, "most feelings of knowing are less dramatic than the Challenger study. We don't ordinarily sense them as spontaneous emotions or moods like love or happiness; rather they feel like thoughts – elements of a correct line of reasoning." These thoughts, regardless of how logically you believe you have reasoned help illustrate how the feeling of certainty creeps into your thinking in a very subtle way. From Burton's important work, you have no volition in choosing the feeling of certainty and importantly the feeling is a blind spot, almost impossible to sense. "Inside the human mind, certainty is a primary mental state driven by emotions and it is completely independent of any underlying state of knowledge or rational thought process regardless of how you feel about this statement." [10]

As an example, many readers have experienced the shock of hearing that a close friend or Soldier in their unit has been killed. The unexpected death does not feel right and we feel that our friend is still alive. It takes time for the bad news to sink in. From Burton's work, "this disbelief associated with hearing about the death is an example of the disassociation between intellectual and felt knowledge." Your feeling of certainty governs thinking and decision making and in fact, every aspect of your life. In the practice of the profession of arms all learning, judgment and decision-making is influenced by the feeling of knowing. Certainty in the mind of Army leaders has profound implications on the conduct of military operations.

The Human Brain

A fundamental discussion of the brain is important because it reveals why "certainty" is an emotional feeling rather than a logical conclusion based on inductive or deductive reasoning as many erroneously believe. The basic principles of neurobiology support this premise. From Dr. Burton's book, the basic brain cell is called a neuron and the typical neuron receives incoming information from approximately 10,000 other neurons through nerve fibers (axons) across a tiny gap called a synaptic cleft. Each bit of information either stimulates (positive input) or inhibits (negative input) cell firing. [11] As you are reading this paper, neurons are firing inside your brain by the billions. In each neuron, when the sum of each of the inputs reaches a critical threshold, an electrical charge travels down the axon to the region where neuro-transmitters are stored. There are a host of control mechanisms which manage this process (mostly enzymes) but neurons are also affected by genetics, disease, diet and importantly, drugs and alcohol. Feedback loops in the brain alter the availability and receptivity of the postsynaptic receptor sites and how cells signal and adhere to one another. [12] Understanding of these regulatory processes and control mechanisms is a major challenge of modern neurobiology and quite beyond the scope of this paper. As Dr. Burton explains:

"Despite the veritable symphony of interacting mechanisms, the neuron ultimately has only two options—it either fires or it doesn't. At this most basic level, the brain might appear like a massive compilation of on and off switches. But the connections between neurons are not fixed entities. Rather they are in constant flux—being strengthened or diminished by ongoing stimuli. Connections are enhanced with use, weakened with neglect…once we leave the individual synapse between two neurons, the complexity skyrockets – from individual neurons to billions of brain cells each with thousands of connections."

The firing of billions and billions of neurons forms the brain's neural network. The neural process is very rapid, extremely small and incredibly complex. It is difficult for those not familiar with neuroscience to imagine the skyrocketing complexity. The enormous number representing the potential neural connections in the human brain, points to an almost limitless capacity for the human being to learn. Much more important than the potential capacity of the neural network is the actual use of the neural connections. The actual neural connections in your brain is a smaller yet enormous number and it represents what you think and in a sense it is who and what you are -- the sum of all you think. The actual use or quality of the neural connections in the brain is important as it represents the difference between a newborn infant and Einstein or between a second-grader finger painting in school and Michelangelo. As you think and learn, the neural connections continually change and sometimes the feeling of certainty also changes. Obviously more challenging than the brain's potential or the quality of neural connections is "unraveling how" individual neurons collectively create thought. Dr. Burton coined this challenge as the 'Holy Grail' of neuroscience.

How Do You Know What You Know?

Burton's book, On Being Certain provides the biological, medical and scientific underpinnings for understanding that feelings and facts are often at odds. The deep-seated feeling of certainty that is separate from any underlying state of knowledge, reasoning or reality is not just driven from feelings but fundamentally it too, is an emotion. Certainty feelings are very much like other emotions such as feelings of love, fear, hate or anger. Reflect for a moment; why are some people so utterly convinced that their position is correct in spite of overwhelming evidence to the contrary? And why do others consistently entertain healthy skepticism? Which are you? Isn't it curious how certain some individuals can be about an outcome or idea when there is no logic, no reason and no facts supporting their position!

The feeling of certainty is a complex neurological process that works itself out largely outside our conscious awareness. Think for a moment of the one belief you feel the most certain about in your life -- you possess the "feeling of knowing" about this conviction and it may very well be true but your certainty is not derived from logic or reasoning. Your feeling of certainty is biologically driven from your senses and basically an emotional feeling. This feeling of knowing coupled with myriad human biases, some of them known but mostly blind spots, represent a significant danger the professional Soldier. The feeling of knowing is a threat to decision-making, coherent reasoning and judgment and consequently to success in military operations. Here are several illustrations resulting in the "feeling of knowing."

A Rose By Any Other Name?

Essence words [13] can be helpful as a shortcut to human communication but can also present a danger. "Postmodernism has long noted that the words we use to communicate really never capture the precise meaning of our thoughts. Importantly, we have no control of the meanings others take from our words." [14] The words we use are essential in our thinking but words are not essential to our feelings, particularly the feeling of knowing. Additionally, words often bias our thinking by how they frame our environment and often deceive us. Words using historical analogy, with references such as Vietnam, Pearl Harbor or 9-11 serve not only to fool us by framing our sense of certainty, but they are particularly effective as they appeal to the

emotion. The Vietnam War cost 58,000 lives and Pearl Harbor was the rallying call for entry into WW II. For the past ten years many “Vietnam-like counter-insurgency” analogies to US Army operations in Iraq and Afghanistan have been offered.[15]

Religion and Politics!

About 85% of the people in the United States profess to be Christian.[16] Christianity the largest of all religious groups and represents well over two billion people worldwide. Islam (1.5 billion), Hinduism (one billion) and Buddhism (500 million) with folk religions in China, Asia and Africa represent about another one billion combined. [17] There are estimated over 38,000 different religious groups on the planet.[18] The largest group, Christianity possesses hundreds of different denominations, sects and groupings. Well over 97% of the people on earth are spiritual in the sense that they are not agnostic, nor professed atheists.[19] Every one of the almost seven billion humans on earth possesses a varying degree of certainty regarding their faith.

For countless millions however this “feeling of certainty” is absolute in that they intrinsically “know” their faith to be true. Ironically, many of these same people who are certain in their faith practice the very same faith that their parents raised them to believe. Many never experience another conviction; they never read other spiritual or religious literature and never considered another point of view regarding their personal faith. The feeling of knowing that goes with the personal faith inherited from your parents may be wrong! Holding to the naive belief that you have logically reasoned or rationally selected your inherited religious views is a feeling of certainty with the illusion of a logical, reasoned choice in your decision. Personal faith for many is biologically driven and emotional determined by your culture and pervasive in the human race.

Moral Intuition and Certainty

So, what makes you “certain” that you see the moral world as it really is? One problem with morality lies in definition. For theologians, philosophers and moralists a definition of morality is really only a feeling, unique to each individual. The concept of morality, like the existence of God and squishy trust or vague leadership concepts are rarely if ever, adequately defined by philosophy or any other system of thinking. Most systems of thinking offer only a weak definition that is ambiguous and controversial. Secular morality, if defined at all, takes the approach of trying to define `moral foundations or systems.' From Professor Haidt, "Moral systems are interlocking sets of values, virtues, norms, practices, identities, institutions, technologies, and evolved psychological mechanisms that work together to suppress or regulate self-interest and make cooperative societies possible."[20] Defining morality in terms of cooperative societies or self-interests or moral foundations is problematic in that without a generally agreed upon definition and purpose, how can we understand, apply and get to a common application of morality to our human relationships? It’s difficult because human beings rarely possess the capability to fully understand their complex feelings and even more rarely, possess words to accurately describe the concept of morality to others. Importantly, we definitely have the feelings of knowing what we believe. Our view of what is moral and what’s not, like the feeling of certainty, is dominated by emotion. Social scientists have demonstrated that moral reasoning is an ex post facto process, directed at moral judgments from emotionally dominated intuition.[21] Said another way, your moral views and choices are feelings of knowing driven by an emotional response and supported by the biases that exist in your mind.

Conclusion

There is no intent to defame anyone’s personal religious, political or moral beliefs. The topics of faith and the politics of morality all seem rampant with certainty. They serve to illustrate how the feeling of certainty and illusion of choice is ubiquitous. The purpose of these emotionally charged examples is to encourage the reader to think and reflect about the “feeling of certainty” in their own experience

Be careful with your feeling of certainty, it can be a deceptive and powerful blind spot. The feeling of certainty originates primarily from your emotions and secondly from your senses. Your emotional feelings are often wrong and as demonstrated what you sense can likewise be wrong! Certainty and similar states of ‘knowing what we know’ are sensations that feel like thoughts but arise out of the involuntary brain mechanisms that function independently of reason and logic. Certainty is a strong feeling, indistinguishable from other powerful emotions such as love, hate, anger and fear. It is particularly dangerous to believe that certainty can be derived from rational human thinking or logical judgment; often your feelings simply validate a wrong conclusion. This knowledge should serve as a powerful tool for Soldiers and especially for commanders. It should help with decision-making, operations, training and learning as well as every activity that involves thought, planning and human relationships.

Moreover, the degree of certainty you hold in your mind, subtly frames and influences your perception of the operational environment. It colors your sense of reality and how you approach planning, problem solving and

decision-making. Empirical evidence, judgment and reason may help but cannot in themselves overcome the neural network's powerful feeling of knowing. The use of critical reflection and collaboration with others, especially divergent thinkers should assist with judgment and decision making. Our decision-making and judgment can benefit greatly from the informed opinions of others. "Red teaming" or antagonistic players should play a fundamental role in the planning of operations. Rely on others to challenge your own gut feeling. Other important advantages with using collaboration; first remember that all bias particularly the feeling of certainty, is a blind spot. We are able to see bias in others better than in our self, especially when it comes to moral or ethical issues. Others can help us to see our own bias better and balance the emotion which dominates our fragile human decision-making abilities and processes. Second, the use of collaboration, particularly a very diverse group, will not only enhance decision-making but will greatly aid in creativity and innovation. Finally, the use of tried and true methods like 'trial and error' and remaining open to new ideas and skeptical of any justification that says, "We've always done it this way."

When faced with 'ill structured' problems, tough decisions and any situation that you are dogmatically certain about – put on your skeptical hat and re-think. It's important to maintain and promote healthy skepticism within yourself and the team, it's an important part of a healthy command climate. Warning: be careful to guard against slipping into cynicism which may be counterproductive and disrespectful. Additionally, don't be afraid to change your mind if subsequent evidence proves your initial 'feeling of knowing' was wrong. [22]

Finally, any stance of absolute certainty which precludes the consideration of alternative opinions, thoughts or ideas is fundamentally flawed and is particularly dangerous in the practice of the profession of arms. Understanding that certainty in your mind is an emotional feeling spurred on by the illusion of choice will help to avoid the "god complex" and many of the dangers it poses to decision making and military operations. By having a healthy sense of skepticism when confronted with "certainty" in the workplace or your personal life, you demonstrate awareness that your brain and body are wired for systematic mistakes and unreliability. Knowing this, you will be become a better leader, decision maker and commander.

"Uncertainty is an uncomfortable position. But certainty is an absurd one." [23] Voltaire.

Author's Note: This work is an abridged version of "Fooled by Certainty" presented at the "Ethics of Vicarious War Symposium," Command and General Staff College, Fort Leavenworth, KS, November 2012.

Notes:

[1] http://thinkexist.com/quotes/mark_twain/ accessed on 18 JAN 2012.

[2] Most readers will call into mind the Salala outpost disaster in which 24 Pakistan Soldiers were killed. http://www.bbc.co.uk/news/world-asia-15901363

[3] Ashby, Nathaniel J. S., Dickert Stephan and Glockner, Adreas, quoted in : " Focusing on what you own: Biased Information uptake due to ownership." Judgment and Decision Making, volume 7, No. 3, May 2012, pp. 254. (See also, Kahneman & Tversky, 1972, 1979, et.al. 1982)

[4] Sevcik, Michael C. Moral Intuition and the Professional Military Ethic, Small Wars Journal, April 2011. See also: Haight, Johnathan, and Graham Jesse, when morality Opposes Justice: Conservatives have Moral Intuitions that Liberals may not Recognize, Social Justice Research, DOI: Springer Science+Business Media, LLC. 2007

[5] Burton, Robert A., M.D., On Being Certain, Believing you are Right Even when you're not, page xiii, St. Martin's Press, 175th Fifth Ave, NY, NY, 2008.

[6] Burton, ibid.

[7] Burton, ibid, see pages 9-12 for a synopsis of the Challenger study.

[8] Haidt, Jonathan, The emotional dog and it's rational tail: A Social Intuitionist Approach to Moral Judgment, (Psychological Review, 2001, Vol. 108, No. 4, 814-834).

[9] Ibid, Page 37.

[10] Ibid, page 41–italics added

[11] Ibid, page 41.

[12] Ibid, page 42

[13] Authors note: the use of "words" here denotes the language we all use to communicate. Words are not limited to discussion and dialog but are an essential part of our thinking.

[14] Brookfield, Stephen, D., The Skillful Teacher, page 249, 2d Edition, Jossey-Boss, San Franciso, CA 2006.

[15] Johnson, Thomas H. and Mason, M. Chris, Military Review, Afghanistan and the Vietnam Template, November-December 2009; page 2. An example: often authors and readers don't have any idea that they are falling prey to loaded words or bias, in this case a "representative" heuristic. On the other hand, some authors know very well and use this heuristic in an attempt to influence their readers.

[16] 33% of the world's population is considered to be Christian. The three largest Christian populations in the world are: USA - 224,457,000 (85%) Brazil - 139,000,000 (93%) Mexico - 86,120,000 (99%), Gordon Cromwell Theological Seminary accessed : 24 JAN 2012 See: http://christianity.about.com/gi/o.htm?zi=1/XJ&zTi=1&sdn=christianity&cdn=religion&tm=27&f=10&tt=11&bt=1&bts=1&st=11&zu=http%3A//worldchristiandatabase.org/wcd/

[17] See: http://www.religionfacts.com/big_religion_chart.htm accessed on 24 JAN 2012 and "World: People: Religions". CIA World Factbook. Central Intelligence Agency. 2007. ISSN 1553-8133. https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html#people.

[18] Ibid, World: People Religions.

[19] Ibid, World: People Religions.

[20] Haidt, ibid.

[21] Haight, Ibid and Sevcik, Michael C. Moral Intuition and the Professional Military Ethic, SMJ March 2011.

[22] Johnson, D.P. and Tierney, Dominic, Crossing the Rubicon: The Perils of Committing to a Decision, Harvard Kennedy School, Belfer Center for Science and International Affairs, Policy Brief, September 2011.

[23] François-Marie Arouet better known by his pen name: Voltaire. http://qwotebook.com/Voltaire/ accessed on 23 JAN 2012.

Table of Contents

One of the Few: The Cultural Support Team

By Capt. Saska Ball, ShadowSpear, 01 September, 2013

FORT BRAGG, N.C - “I packed up my whole life. It’s all in storage right now so, if I didn’t make it through selection, I was literally not going back to anything,” said Staff Sgt. Rachel Fisher of the 448th Civil Affairs Battalion based at Joint Base Lewis-McChord, Wash., and resident of Anacortes, Wash.

Fischer was one of 85 soldiers, and one of four with the United States Army Civil Affairs & Psychological Operations Command (Airborne), who went through a 10-day assessment and selection process for a chance to attend a female-only program taught by the United States Army John F. Kennedy Special Warfare Center and School located here.

In its sixth class iteration, the Cultural Support Team program fills an important role within the Army’s special operations community.

“The CST course was developed to fill a need and requirement that two units essentially had,” said Sgt. 1st Class Christopher Barnes, CST Chief Instructor. “One being for the direct action assets, or surgical strike teams. The Ranger Regiment needed females on the battlefield to search women and children when they went into the objective. The other side, the special warfare side, the village stability operations, Special Forces groups and Marine Corps Forces Special Operations Command needed females to interact with the female populace.”

Fischer first heard about the CST program from a fellow soldier while she was working as a subject matter expert at the civil affairs reclassification course in early 2012.

In November 2012, after obtaining her master’s degree in conflict archeology at the University of Glasgow in Scotland, she returned to the U.S. and applied for the CST program.

“They tell you it’s a physically demanding course and to be prepared mentally but they don’t tell you what to do,” said Fischer. “I kind of went with what I knew I needed to improve on personally, which was PT [physical training], and kept an open mind about everything else.”

In anticipation for the physically and mentally challenging selection process, Fischer prepared by hitting the gym for two hours a day and doing online army courses.

“I did a lot of PT! Mobility, cardio and regular strength training,” she said. “I read up a lot on the basic soldier skills and just knowledge about Afghanistan. I don’t think I could have prepared any differently.”

Out of the 85 that showed up for assessment and selection, only 37 were selected to attend the five-week cultural support training course.

“Going to selection was the first time I walked into a situation and couldn’t really prepare for it but you knew it was something that was going to test everything you had,” Fischer said. “Passing selection was the moment I said, ‘Wow! I can really do this!’”

Following assessment and selection, Fischer and the other females chosen to attend the CST training course began the classroom portion where they were taught everything it takes to be a successful member of a CST.

The CST training focused on the duties of a cultural support specialist, which is primarily engaging with the local population. The foundation of the CST training is built upon providing an understanding of human behavior, an appreciation for Islamic and Afghan culture and the role and history of women in Afghanistan.

In the classroom they learned about their role as a SOF enabler, their mission, how to use an interpreter, conduct tactical questioning, and become an adaptive thinker. Outside of the classroom they became familiar with the M4 carbine rifle, M9 pistol, medical training, how to conduct searches of people and buildings and moving as a team.

“My civil affairs experience has helped me a lot,” said Fischer. “I’ve had previous experience using interpreters, both good and bad. It has also helped a lot interacting with other cultures because I’ve done a lot of sit down meetings and interacting with people when I was deployed to Iraq. I’ve learned how to maneuver around different cultures, politics and religious views and still at the same time accomplish the mission.”

Aside from bringing her personal experience to help her through the course and applying what she learned from the classroom portion, there are also subject matter experts assigned to the CST program to provide assistance and real world experience.

“We’re here to basically give them an understanding of what we did downrange and some of our tactics, techniques and procedures that actually worked for us and different ways we were able to engage the population, whether it be male, female or adolescent,” said Master Sgt. Susan Letendre, who was a graduate

of the fourth CST course and who recently returned from a deployment where she was attached to two operational detachment alpha teams in Afghanistan.

The final portion of the CST course is a comprehensive field training exercise.

“For the past few days we’ve been running through the surgical strike and special warfare lanes being tested on the skills we’ve learned so far,” said Fischer. “Basically it’s about building rapport and gathering information. They give us targeted goals and we try to achieve those goals within a time limit without insulting the people and their culture.”

“Staff Sgt. Fisher is one of my students,” said Sgt. 1st Class John Walker, CST team 2 small group instructor. “She’s doing very well. She’s taking what she knows as a 38B, civil affairs specialist and applying it to the scenarios along with her 68W, health care specialist background. She’s taking all of her skill sets and applying them into the course.”

Upon completion of the CST course, soldiers are awarded a professional development skill identifier and title of cultural support specialist. Those selected for a deployment are chosen to support one of two missions. They can be attached to a Ranger element to support the surgical strike teams or to a Special Forces element to support the special warfare mission.

Fischer completed and graduated the CST course, becoming only one of 13 female soldiers in the Army Reserve, and one of three in USACAPOC(A) to hold that distinct honor. She was selected for the Special Forces mission and will return to Fort Bragg, N.C., this fall to complete pre-mobilization training with 3rd Special Forces Group, followed by a deployment to Afghanistan.

“It’s been a great experience,” said Fischer. “It’s been really challenging but fun at the same time. I’ve learned a lot and I’ve improved on skills and learned whole new ones. I can’t wait to put them into play.”

Table of Contents

Voice of Russia Is a Great Contributor to Freedom Of Expression – British MP

By Evgeny Sukhoi, Voice of Russia, 4 September 2013

As the Syrian conflict continues to spiral beyond a diplomatic solution, the UK has joined the White House in claiming Damascus had used chemical weapons on its own people. It has recently emerged that some members of the UK parliament have been shaming opposition MPs for re-tweeting Voice of Russia articles on Syria that look at the issue from a different angle. Brooks Newmark, a member of the British Parliament since 2005 and expert on Middle East economic and foreign policy, has called the Voice of Russia a great contributor to freedom of expression that provides a wide range of opinion, but disagreed with the stand it has taken on Syria.

Don’t you think it is quite unreasonable for the Assad regime to use chemical weapons firstly because they are stronger at the moment militarily and secondly that they used just a small portion of these chemical weapons, it didn’t have any sense. What is your impression on that?

Nothing in warfare is ever rational and if you look at the circumstances, certainly in my understanding in the circumstances in which this particular attack took place, it happened just after Bashar Al-Assad’s family was attacked by opposition forces in a convoy, effectively when they were breaking the fast after Ramadan. Bashar Assad’s brother Maher is responsible for defending Damascus. I think he viewed that as an incredible humiliation and notwithstanding the presence of the UN inspectors he just said “I am going to do whatever is necessary”. You and I are perfectly rational people and we may think it is an irrational response but, as I said, I don’t think the members of the Bashar Assad regime and his family are particularly rational human beings.

You described Russia as a key supporter of the Assad regime. But Russia is not alone in opposing military intervention in Syria: more than 10 countries have spoken against the idea. Would you please comment on this?

Sure, there is another 190 countries that are on the other side. I mean you are in an isolated minority in Russia with maybe the North Koreans and Iran, the Chinese and maybe a few others on your side. Unfortunately, on this particular battle you are morally on the wrong side of the argument. I wish that Russia played a more constructive role. I have huge respect for Mr. Lavrov. I think he is a bright intelligent man.

Is it true that you put some opposition MPs to shame for re-tweeting articles on Syria from the Radio VR website. Did you find something outrageous in our coverage of the Syrian crisis?

I think you, as a news media outlet, provide a wide range of opinion. Unfortunately, when you spread the disinformation spread by both Mr. Putin and Mr. Assad, that they deny any responsibility for the weapons

attacks that took place 10 days ago, and say it is more likely to be the opposition – to me that was morally beyond the pale to say that.

When asked about Iraq, Mr. Newmark said:

I don't want to talk about Iraq, I want to talk about this situation. Don't conflate 2 issues. Iraq is a very different situation in which we should never had got involved.

Why should we retranslate the position of media outlets that gave that lie of the US back then and hold them legitimate for their information and hold illegitimate another media who gives some other views and comments which you hold disinformation when we know it was disinformation as well back then?

I was not in Parliament then and I can only talk about what is now. I think the experience of Iraq, where unfortunately intelligence was doctored by Mr. Blaire, led to a bad decision to go into Iraq where we should never have gone there. I am going to agree with you on that point. And by the way there were no weapons of mass destruction in Iraq.

As we know the analysis, the samples of chemicals have just been delivered to Sweden to the laboratory. Why not wait and why not analyze the information a bit more thoroughly before making the final decisions?

I think that is exactly what is going on now. I think that the UN is, number one, reaffirming whether chemical weapons were used or not and unless someone's been living in a dark cave, I think everybody knows that chemical weapons were used. What those chemical agents were, I am more than happy to hear other parties do their analysis in addition to the UK, France and the USA who have done their own analysis on the samples that have been smuggled out. So, I am not going to disagree with you on that point.

In general we know those conflicts and those campaigns in Afghanistan, in Iraq, in Libya. Do you really think that after those invasions and those campaigns the situations in those countries got better?

The answer to your question is probably no. I think in those situations that for many people things have gotten worse. But I prefer to look at this as more like the Balkans, like Bosnia and Kosovo, which were humanitarian crises on a massive scale. Just because the geographic proximity of Syria with Iraq and elsewhere that we've gotten involved in, one shouldn't mix up the two different situations. In my view this is a massive humanitarian crisis where the UN, and I wish the UN would take action, has an obligation and the right to protect. If the UN fails to live up to that because unfortunately Russia with China keeps blocking through their veto any action or any condemnation of the Assad regime, as in the Balkans we have to think of other ways to try and come in and deal with this humanitarian crisis.

Thank you for your opinion. As you see we let you say whatever you want. We are not blocking that.

Thank you very much for that.

And please don't ban your colleagues from re-tweeting things from our website.

I just think it is a shame that they were only re-tweeting what you were saying and not actually listening to what our own side of the argument was saying. I believe in freedom of expression and certainly your outlet is a great contributor to freedom of expression and I support you.

Table of Contents

US and Turkey to Create Fund to Stem Extremism

By Eric Schmitt, New York Times, September 27, 2013

WASHINGTON — The United States and Turkey on Friday will announce the creation of a $200 million fund to combat violent extremism by undercutting the ideological and recruiting appeal of jihadists in places like Somalia, Yemen and Pakistan, State Department officials said Thursday.

While the United States and its allies in the global campaign against terrorism have over the past decade effectively honed their intelligence and reconnaissance skills to hunt terrorists, the West continues to struggle in its efforts to prevent the process of radicalization that creates them.

The new fund, formally called the Global Fund for Community Engagement and Resilience, will for the first time combine financing from both government and nongovernment entities to identify credible local organizations; develop, monitor and evaluate programs; and channel funds to local projects that target groups and individuals vulnerable to appeals from terrorist groups.

It is expected to be operational by mid-2014, officials said.

The initiative, based on other global funds to combat AIDS, malaria and tuberculosis, is to be announced by Secretary of State John Kerry and Turkey's foreign minister, Ahmet Davutoglu, at a meeting of foreign ministers of the Global Counterterrorism Forum in New York. The United States and Turkey are leaders of the

group, an organization of 29 countries and the European Union created two years ago with the State Department's support to act as a clearinghouse of ideas and actions for civilian counterterrorism specialists.

"Countries that have a radicalization problem previously had to rely on ad hoc support from wealthier donor nations, many of which are not bureaucratically capable of sponsoring the small intervention programs necessary to disrupt the radicalization process," said William McCants, a former State Department counterterrorism official who is now a fellow at the Brookings Institution. "Now countries can turn to the global fund to sponsor programs that will pull young men and women back from the edge of terrorist violence."

The United States is initially expected to contribute $2 million to $3 million to the fund, which will be administered in Geneva. Other likely donors besides Turkey include the European Union, Canada, Qatar, Denmark and Britain as well as private sources. American officials said they expect the fund to raise more than $200 million over a 10-year period.

Grants from the fund would provide vocational training to youths at risk of being recruited by terrorist organizations; new school curriculums that teach tolerance and problem solving; and Web sites and social networks to educate youth about the dangers of violent extremist ideologies.

The new fund builds on other efforts the counterterrorism forum has promoted including the creation of a center in Abu Dhabi to counter violent extremism.

Denmark has already forged a partnership with Burkina Faso to respond to violent extremism in the Sahel region of Africa, and backed it up with a war chest of $22 million over five years. Separately, Saudi Arabia announced last month that it would donate $100 million to the United Nations Center on Counterterrorism. American officials have suggested that the United Nations give some of the Saudi money to the new fund.

Although countering violent extremism is a policy priority for the United Nations, it does not have the ready ability to provide financing to small grass-roots organizations that do that work, American officials said. Thus, providing money to the fund would allow the United Nations to support an important counterradicalization effort, the officials said.

On Friday, Mr. Kerry is expected to explain that radicalization is often fueled by conditions at the local level and that there is no one-size-fits-all approach to countering violent extremism, State Department officials said.

Citing recent terrorist attacks in Kenya and Pakistan, Mr. Kerry will note that communities are at the heart of any solution in combating this threat, and that authorities must tailor responses to conditions in those communities.

American counterterrorism officials say that the most enduring anti-extremism programs are those owned and carried out by local civic and government partners.

Table of Contents