Information Operations Newsletter

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

ARSTRAT IO Newsletter Online

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

Table of Contents

Vol. 13, no. 03 (December 2012)

Why Your Intuition about Cyber Warfare is Probably Wrong

By Matthew Miller, Jon Brickey and Gregory Conti, Small Wars Journal, Nov 29 2012

Since the dawn of time, when one caveman first struck another, humans have relied on a natural understanding of their physical environment to conduct warfare. We have an inborn ability to understand the laws of the physical world. In order to shoot an artillery round farther, just add more powder; to provide cover for protection against bullets, hide behind a rock. A private might accidentally shoot the wrong target, but the potential damage is limited by the maximum range of his or her rifle. The laws of physics, however, are counterintuitive in cyberspace. In cyberspace, our understanding of the "laws of physics" is turned on its head. Weapons can be reproduced instantly, "bullets" travel at near the speed of light, destroyed targets can be brought back from the dead, and a seventeen year old can command an army. As human beings we are at a distinct disadvantage when thinking intuitively about cyber warfare. In this article we study where our intuition fails us in cyber warfare and suggest alternate ways to think about the conduct of cyber war that account for the vast differences between the kinetic and the non-kinetic fight. A correct understanding and appreciation of these differences and common misconceptions is absolutely necessary to conduct cyber warfare and to integrate cyber effects into the kinetic battlefield. To ground this work we need to define the term "cyber." There is significant and evolving debate regarding the precise definition of cyber. For purposes of this article we define cyber as a spectrum of cyberspace operations including Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND).

The Attacker has the Advantage over the Defender

In classic military doctrine, the defender has a distinct advantage over the attacker. In today's model of cyber security, defenders build layers of defenses to protect the confidentiality, integrity, and availability of critical assets. Security professionals pour millions of dollars into such defenses, but with only limited success. A Maginot Line strategy rarely works in cyberspace because attackers need only find a single flaw to launch a successful attack. Perfect defense is impossible; the astronomic complexity of the software and hardware woven into our information systems and networks is beyond human comprehension. As an example, the Windows XP operating system alone has more than 45 million lines of computer code, creating an immense attack surface. Many aspects of computer security cannot be solved by computers, such as determining the exact operation of a piece of untrusted software. Attackers however, can probe these complex systems to find a flaw and are frequently successful. Hardware and software monocultures, such as widespread use of a single operating system or web browser, amplify the impact of these discoveries by facilitating widespread compromise. Against a determined adversary, many security experts believe we cannot keep our computers secure, compromise is simply a function of time and dedicated resources. Common defenses, such as antivirus systems are reaching the end of their usefulness and cannot be relied upon for effective defense. Even air-gapped networks, not directly connected to the Internet, have proven vulnerable to mobile malicious code. Recent research indicates that defenders must field 1,000 times the resources (money, people, time, compute power, etc.) to reach parity with attackers in cyberspace; this is not a winning proposition for the defender.

We aren't Fighting the Krasnovian Army

During the Cold War, military planners could rely upon relatively fixed threat doctrine, see Figure 1. We knew the capabilities of threat units and could plan accordingly. In the cyber domain, threat Tactics, Techniques and Procedures (TTPs) are constantly changing. One day we may have a distributed denial of service attack, the next day a phishing attempt. We could also have a drive-by download, a USB stick dropped in a parking lot or something else entirely new. The list goes on and on because new capabilities and TTPs are developed on a daily basis. Adversaries include well-resourced nation states and large online criminal organizations; however, even small groups and individuals can join the fray and have a tremendous impact. In some ways we are already at war. We have much to learn by studying insurgency and applying those lessons in cyberspace.

Reserve Forces may be more Capable than Active Duty Troops

In kinetic operations, reserve forces have always been at a distinct disadvantage, often equipped with older equipment and less frequent training opportunities. However, reserve personnel are at their best when their civilian careers match their military roles. Truck drivers are a textbook example. Great opportunity lies for the military to recruit Reserve and National Guard personnel who are experts in cyber security; and we need to. The high churn of active duty forces between assignments inside and outside cyber continually degrade their skills. Embracing the value of reserve cyber experts, and civilian cyber experts, bears great promise for the future cyber workforce.

A Computer Can Be Turned into a Brick

Cyber Attacks can have devastating real world effects. We tend to think in terms of lost or corrupted data as a result of an attack, however computer hardware can be destroyed, or "bricked," by corrupting its internal firmware and other means. This happens fairly rarely today because many malicious applications are tied to online crime and avoid harming their host. However, we should assume that our adversaries in a time of war will not be reluctant to destroy our information systems, weapon systems, and our Nation's critical infrastructure, including financial systems. Beyond just disabling or destroying computer hardware, software, and data, malicious software can also cause significant physical damage. Experts have warned of vulnerabilities in the SCADA systems which control water, power, communication, transport, and manufacturing systems. Stuxnet provided a very clear example of such capabilities by reportedly destroying centrifuges used to enrich uranium. We shouldn't forget that our weapon systems are heavily reliant on computer technology and may be vulnerable. The recent virus found in a military drone command center may be a warning of things to come. Our military depends on its technical advantage. If we lose our communication and information processing systems we will be severely degraded as a military and possibly rendered combat ineffective.

Cyber Terrain is more like a Parallel Dimension than Physical Space

We have been navigating physical terrain since birth, but networks aren't physical space. Cyberspace crosscuts the physical domains of air, land, sea, and space, and touches at myriad points. Networks aren't physical battlefields. Attacks can transit the globe at near the speed of light. Battles can be won or lost in milliseconds. In this virtual world, distance approaches zero. Enemies can teleport, appearing from numerous locations around the globe in the blink of an eye. Cyberspace is a man-made domain, it is constantly shifting as new nodes are added and others disappear. Grid squares can move (by changing a network address) or lie (spoofing a network address). Laws and military doctrine were written with physical boundaries in mind, but national borders in cyberspace are intertwined in complex ways unanticipated by the law. Unit boundaries, measured in kilometers of dirt are frequently meaningless. A cyberspace attacker may instantly appear in a brigade operations center in Afghanistan or a game console in New Jersey.

Adversaries Can Easily Camouflage, Deceive or Disappear

Deception is easy on the Internet. Identities can be spoofed or stolen. Age, date of birth, gender, appearance, and marital status are all malleable. Adversaries can operate invisibly or leave little trace behind by cleaning logs. Attackers may disappear and reappear instantly on the other side of the world, by simply changing network connections or paths.. History itself may even be rewritten by altering system log files or other data. The nature of the Internet allows many people to share the same identity (by sharing the same authentication credentials) and one person to appear as many (by creating numerous user accounts). Trust is often misplaced. The end result is that is that things aren't necessarily what they might appear to be in cyberspace.

The Law of War and Cyber Policy Cannot Keep up with Technology

The law of war is well understood around the world and briefed to every service member. The law of cyber war is unsettled. Most legal professionals and judges have limited understanding of technology. One leading cyber warfare legal expert describes the situation in stark terms – explain technology to lawyers at the third grade level and to judges and juries at a first grade level (Clark's Law). Of course, technically savvy legal experts and policy makers exist, but the rapid advance of technology guarantees law and policy will lag years, if not decades, behind what is technically feasible today. For the foreseeable future, military leaders will be constantly challenged with navigating this legal and policy morass and petitioning policy makers for updated laws.

Your Weapon Systems May Work Once, Twice, or Not at All

If you've seen Star Trek, you are probably familiar with the Borg. In numerous episodes the Enterprise crew attempts to defeat borg drones by calibrating their phasers. However, the Borg quickly adapt and the phasers are no longer effective. The same holds true for cyber weaponry.

We see this cycle repeated on a daily basis. New vulnerabilities and exploits are discovered and weaponized, but once used or disclosed vendors will patch systems, antivirus companies will issue new signatures, and security professionals will develop countermeasures. Unlike our M16's, we cannot be assured that cyber capabilities will work after first use, if at all. The result is an ongoing cyber arms race and a burgeoning malware economy to acquire newer and better techniques.

Any Sufficiently Advanced Technology is Indistinguishable from Magic

Without an understanding of technology and networks, computers are just magic black boxes that sit on our desks. In the kinetic realm, warfighting leaders are developed over decades of developmental assignments, operational experiences, and training programs that are among the best in the world. While work is ongoing to develop cyber career paths, we are in the early stages. At the same time, there is a common misconception that "leaders are leaders" and that anyone can effectively lead cyber warfare units. Cyberspace is a new operational domain, and as we have tried to illustrate in this article, many of our instincts are wrong. The generalist leader model, where everyone is replaceable, may work within an operational domain (Air, Land, Sea, Space, Cyberspace), but leaders forced into other domains are at a distinct disadvantage, at best. There is a reason why we don't place Army officers in charge of aircraft carriers. That being said you go to war with the Army you have, not the Army you wish you had. We need to fight to understand the domain of cyberspace and learn to effectively lead cyber warriors.

A Seventeen Year Old can Command an Army

Adversary leaders in cyberspace need not be seasoned fifty year old General Officers, and unless they are part of a traditional nation-state military organization, they almost certainly will not. Adversary leaders will likely emerge based on merit and possess significant experience online. Some will possess traditional schooling, but others will be self-taught and may have tapped the exceptional free resources available online from organizations including Wikipedia and Khan Academy, even MIT or Stanford. Some will have experience in leading distributed teams, possibly Clan Armies in online games and virtual worlds. Their weapon systems can be actively controlled or passively controlled via pre-programmed logic. Lawyers won't be involved (a major agility advantage), and organizational structures will be more like a fluid New Model Army than a rigid hierarchical organization. As a result, adversaries will be very agile. The command post, where a commander monitors maps and receives briefings from their staff to make decisions often has little utility when fighting in the cyber domain. The speed of decision making required is beyond human capacity. In an era where a network packet can travel around the globe in milliseconds carrying an attack payload, by necessity, algorithms will increasingly do much of the fighting. Future cyber warfare will be far more like high-speed trading on Wall Street than briefing the commander on potential courses of action.

You Can't Fire Cannons at the Internet

The infrastructure of the Internet is remarkably resilient. The ability to route around physical destruction is built into the Internet's design. There is no Internet kill switch, but there are certainly weaknesses that could be exploited by a determined adversary to disrupt its proper function. When we move above the physical and logical infrastructure planes which comprise the Internet, we should think in terms of specific end users and computing systems. Spear phishing via email accounts has long proven to provide precise means of targeting end users. Drive by downloads of malicious software hosted on compromised websites is another well known way to target users. Social networking sites are yet another means of spreading malicious software and targeting users. Attackers can destroy companies overnight by humiliating leaders or stealing intellectual property. However, as we've discussed elsewhere in this article, false identities can be easily created, complicating targeting. Attacks also bring the real possibility of collateral damage and limited effectiveness. For example, data can be replicated on multiple servers in various locations around the world, so even a successful attack may be quickly negated as a mirror-image of the server is brought online.

An Enemy Combatant can be the Digital Picture Frame at Grandma's House

In cyberspace virtually any computing device is a potential threat or ally. The rise of the Internet of Things, where many physical items will include computer processors and network connectivity, means we will face many potential combatants in cyberspace, see Figure 2. These devices may be compromised during design, manufacture, or anytime thereafter. Imagine if attackers discovered a flaw that allowed successful compromise of a common gaming console. We could be fighting an Army of tens of millions of PlayStations. This scenario isn't out of the realm of the possibility; botnets of more than one million hosts exist today. Research indicates that bot armies can be rented for as little as nine dollars an hour. Your next combat kill may be a robot or a refrigerator.

You Probably Won't Know Who is Shooting at You

In Internet combat you likely won't know who is shooting at you. Anonymity was built into the design of the Internet. Network traffic is comprised of packets that need only a source address and a destination address. Theoretically, the source address would be that of the attacker and the destination address would be the target. In reality, the source address can be easily spoofed and set to any network device anywhere in the world. To blindly return fire, you could, and most likely will, hit an innocent. Even if the source address is accurate, the attacker could have routed the attack through numerous intermediary nodes, some of which are

in the United States, in allied countries, or in countries with no desire to help the US military. In most cases, attribution requires tedious step-by-step analysis—walking back node-by-node to the attacker—and patience to cope with legal and bureaucratic barriers at every turn. There are even anonymity networks that are designed to protect against such attribution attempts that are remarkably resistant to analysis. Note that these anonymity networks, and the design of the larger Internet, were designed to allow open sharing of information, not to facilitate cyber warfare attribution. As a result, accurately identifying aggressors may take weeks, months, or even prove impossible.

Information Wants to be Free

Digital information is slippery. Even the most aggressive attempts at limiting disclosure are not foolproof. Previous attempts at censoring communications, see Figure 3, look quaint in an era where an easily concealed 20 dollar thumb drive can hold 21 million pages of text. Encryption provides an all but impenetrable layer to mask malicious activity. Military censorship is an uphill battle that will only catch a few honest or inept people; true threats will likely take much longer or may never be detected. Censorship attempts also have a counterintuitive secondary effect—they often make the information more available. Coined the Streisand effect, attempts to remove information from the Internet tends to increase proliferation. For example, attempts to prevent dissemination of Wikileaks data (that was widely available online) only drew additional attention to the disclosure and prevented law-abiding Department of Defense personnel from studying the documents. To compound the problem of information disclosure, social networking sites entice disclosure of sensitive personal information from government employees and service members, opening the door to misuse.

Calling for “Cyber Support” is not the same as “Calling for Fire”

There is a trend now to consider cyber operations as being analogous to artillery fire missions. Fire missions are straightforward: get on the radio, pass along target grid coordinates, and moments later artillery rounds come raining in. The same isn’t true for cyber operations. As we’ve discussed earlier, cyber weapons aren’t guaranteed to work and even if they do their controllers may be reluctant to expend them against many objectives. Targeting is difficult and may span multiple countries, far beyond the sector of a tactical unit. Even a single bit in error could result in collateral damage. While details of government cyber operations are not publicly available, civilian red team and penetration testing operations require extensive, time consuming planning. The murky law of cyber warfare compounds the problem, whereas the law of kinetic warfare is largely settled. Lawyers will be involved in cyber warfare, and you can be certain the timelines of many cyber operations will rarely approach the responsiveness of simple artillery fire for the foreseeable future.

Like it or not, Geeks are Warfighters

Cyberspace is the domain of technical experts, in some ways a hybrid of traditional Signals Intelligence and Communications domains, but in other ways altogether different. This cultural shift is uncomfortable for many. Technologists have historically not fared well in the military. Those with technical expertise may be reluctant to lead, lest their skills atrophy, and those without technical skills may not like the shift in power and status to the technologists. Human resources processes are a significant part of the problem. Military human resource systems were designed for interchangeable personnel in well defined specialties. Current guidelines in the Army require frequent moves and check-the-block career progression. Manning documents are based on outdated and slow-to-evolve specialty codes. Given the critical shortage of cyber security professionals, restrictive manning documents artificially constrain available positions to only a small, and often ill prepared, percentage of the force. One potential solution is the creation of a Special Forces-like model where candidates can be rigorously assessed and the best can be selected from across the force.

Conclusions

Cyber operations, alone or in concert with traditional kinetic operations, are intrinsic part of all future warfare. This article was designed to highlight how our physical world instincts often fail us when thinking about cyberspace. Cyberspace operations present both a critical national threat and a significant advantage to the defense of our country. By better understanding cyberspace and its laws of physics we will be better prepared for both.

Comments

.by Robert C. Jones | December 2, 2012 - 7:03am

My intuition about "cyber warfare" is that cyber is a domain where warfare can be waged, like land warfare or maritime warfare or air warfare.

My intuition about "cyber warfare" is that much of our defense against attacks in this domain fall in the realm of civil and commercial due diligence. Just standard cost of business precautions one must do in order to operate in that cyber domain. Airlines assume tremendous costs to ensure they can operate in a reasonably safe manner. Airlines could be far more profitable is they ignored those costs altogether, or could get some government agency to bear the burden of those costs on their behalf.

My intuition about "cyber warfare" is that the idea of calling this "warfare" and creating a Cyber Command and taking this mission primarily into the Defense Department will rob critical resources from other aspects of national defense that actually rely on military capability to be performed. That is not particularly smart. I think we should look to how we handled the opening of the Space Domain. Yes, much of our national defense required developing both offensive and defensive capabilities to optimize advantages and mitigate military risks within this new domain. A percentage of the military budget went to this new domain, reducing the percentages to all other domains by that amount. But as a nation we created a new civil agency, NASA, who had the lead for the space domain. Not everything NASA does goes toward our national defense directly, but indirectly they have provided the majority of the space capacity that DOD relies upon. By creating NASA we in effect expanded our defense capacity without either robbing from or adding to our defense budget. This is smart. As the Defense budget prepares to take a big hit we need to press for the creation of a civil Cyber agency to play the role for that domain that NASA has played for the space domain.

My intuition about "cyber warfare" is that not all violence or all forms of attacks are "warfare." Who commits the act and why they commit the act are critical factors, the nature of the act is interesting, but not the decisive factor. If an individual or even an organization (such as AQ) attacks the power grid in New England trough the cyber domain, it is most likely a criminal act. If a state commits that same act is it most likely an act of war. We need to be careful that we do not allow an over-militarization of our national cyber capacity lead us to a place where we begin to see all such attacks as "war" or "warfare." They aren't.

My intuition about "cyber warfare" is that our military needs to be able to maximize the cyber domain for the conduct of all manner of warfare, from very regular to very irregular - and that we need to be able to conduct all of our missions across that same spectrum even when, for whatever reason, our own cyber-based capabilities are denied. To me, this should be the primary focus of Cyber Command. Let the new civil cyber agency worry about taking lead on the rest.

Those are my intuition about "cyber warfare" - but as the authors point out, I am probably wrong.

.by Bill M. | December 1, 2012 - 10:40pm

Overall a good article, but despite learning a bit from reading this I also disagree with some of the points the authors made. For examples the laws of physics are laws of physics and I see no evidence they have been turned on their head. Just because a weapon can be produced faster doesn't mean a law of physics' has been violated. It simply means we're constantly developing upon our knowledge base and using that knowledge more effectively.

The authors tend to use military lexicon where it isn't appropriate, which is common in our ranks. We now call money a weapon, when in fact money is money, and money can be used to influence a variety of outcomes, and we can wage economic warfare, but that doesn't make money a weapon any more than information in itself is a weapon. Both can influence desired outcomes, but are they weapons? Is that the best way to think of them, or does using that paradigm limit our view of how these means and ways can be employed? On the other hand a virus, worm, etc. that causes damage should it be categorized as a weapon? In this case they're information packets (instructions) that are intended to harm. I think this gets after the author's point about lawyers and judges being behind the power curb.

I think the authors are wrong when they said military planners could rely on a relatively fixed threat doctrine. This is a typical conventional army view because much of the Army was focused narrowly on the Fulda Gap scenario, yet the Cold War was never waged there, it was fought globally and in many regards the threat doctrines were the same type of irregular war we're fighting now, and there was even some cyber operations employed (before cyber was cool). TTPs have always been constantly changing throughout history, but that doesn't invalidate their important point that TTPs are also constantly evolving in the cyber domain, and perhaps at a much faster rate than we're accustomed to.

The human resource management challenge they address is very real, but perhaps especially crucial for so called cyber warriors. Perhaps the best answer is not to have uniformed service members do this, but to recruit DOD civilians. The only military grade that allegedly allows a service member to focus on their technical specialty is the Warrant Officer, but the reality is the Warrants have relatively recently pursued a management system that too closely parallel's regular officers by creating a check the block career path. Why can't we use civilians as our cyber warriors? Reservists don't fit the bill if the assumption is we can suffer a cyber-attack at any time (and the authors give numerous examples of what could happen). Can we really afford to wait for a response until we can mobilize the reservists?

I think the authors could have strengthened their article by adding how Autnomous [sic] employs cyber operations and how the Russians employed it in Georgia. Those are the not the end all, be all examples, but these examples and others would add further urgency. Despite the minor critical comments I made, I thought it was a great article.

Table of Contents

Pentagon Drops 'Strategic Communication'

By Tom Vanden Brook, USA TODAY, Dec 3, 2012

WASHINGTON - The Pentagon is banishing the term "strategic communication," putting an end to an initiative that had promised to streamline the military's messaging but instead led to bureaucratic bloat and confusion, according to a memo obtained by USA TODAY.

Strategic communication had aimed to synchronize the military's messages with its actions. Instead, it led to creation of offices and staffs that duplicated efforts of traditional public affairs offices, according to the memo.

In the memo, Assistant Secretary of Defense for Public Affairs George Little wrote that over the past six years, strategic communication "actually added a layer of staffing and planning that blurred roles and functions of traditional staff elements and resulted in confusion and inefficiencies."

In the Army, for example, personnel assigned to strategic communication slots increased from seven in 2006 to 38 last year, Pentagon records show. The Army spent $5 million for contractors assigned to strategic communication.

Little's memo to the chiefs of the military's combatant commands said, "We avoid using the term SC to avoid confusion."

Strategic communication has had high-level detractors, including Adm. Michael Mullen, the former chairman of the Joint Chiefs of Staff, who said the military communicated more with its actions than messages crafted by strategic communication staffs. Mullen told USA TODAY last year that he preferred traditional public affairs offices to provide information and context on military actions.

The military has struggled for the past decade with its strategic communication. In 2001, an advisory board to the Pentagon was advised that it needed to do more to shape public opinion. Since then, several problems surfaced. In 2009, for example, the military severed a contract with the Rendon Group, a strategic communication firm, after it was learned that the company was profiling reporters who might write negative stories.

Table of Contents

European Renewable Power Grid Rocked By Cyber-Attack

Published on EurActiv, 10 December 2012; Updated: 12 December 2012

A German power utility specialising in renewable energy was hit by a serious cyber-attack two weeks ago that lasted five days, knocking its internet communications systems offline, in the first confirmed digital assault against a European grid operator.

Background

A smart grid is an upgraded electricity network utilising two-way digital communication between producer and supplier, 'intelligent' metering and monitoring systems.

Smart grids offer clear environmental, social and economic advantages but their dependence on computer networks and the internet makes them acutely vulnerable to cyber-attacks, according to the EU's European Network and Information Security Agency (ENISA)

A 2012 ENISA report offered 10 recommendations for protecting grids from cyber-threats, including:

- An improved EU and member state regulatory and policy framework
- The development of a minimum set of security measures by ENISA, in collaboration with member states and the private sector
- Security certification schemes for smart grid components, products and organisational security
- Empowering the Consortium for Electric Reliability Technology Solutions to advise on cyber security incidents affecting power grids

"It was a DOS ('Denial Of Service') attack with a botnet behind it," Boris Schucht, the CEO of 50Hertz told EurActiv on the fringes of a Brussels renewables conference. "It blocked our internet domains so that in the first hours, all email and connectivity via the internet was blocked."

DOS attacks involve thousands of requests being sent to a server each second to clog up a system's functioning.

Electricity supplies were not affected in the onslaught, which was "serious but not dangerous," Schucht said. Email services were quickly repaired, although a fix to the problem was only discovered five days later.

EurActiv has learned that the security breach has already been discussed at an assembly meeting of the European Network of Transmission Systems Operators for Electricity (ENTSO-E), which brings together bosses of the continent's transmissions industry operators (TSOs).

The association is understood to be communicating closely and regularly with the European Commission about potential cyber-security threats to Europe's grids.

However, beyond flagging their critical systems protection working group, ENTSO-E will not comment on the details of particular incidents like the 50hertz attack, or even whether similar attacks have occurred before.

A recent report claimed that one in four of the world's power companies had suffered extortion from criminals who had gained access to their system's utilities.

Cyber-attacks on power grids have the power to disrupt critical electricity infrastructure and until now have been the stuff of science fiction, with a gallery of villains stretching from criminals and rogue states to cyber-terrorists.

The US National Academy of Sciences said last month that a terror attack on the US power grid could cause thousands of deaths and cost hundreds of billions of dollars.

Pointers to Moscow and Kiev

While the identities of the 50hertz hackers are unknown, their cyber barrage was mounted from IP addresses in Russia and the Ukraine, EurActiv understands, although these could themselves have been used to disguise the real source of the attack.

"It shows that we have to take cyber-security seriously," Schucht said. "We have to think how we can best protect ourselves in the future."

50Hertz is one of Germany's four transmissions systems operators, and supplies more than 18 million people with electricity largely sourced from 'volatile' renewable energies like wind and solar.

These account for 38% of 50hertz's production-side energy – and more than half of its capacity – making it the world's leading renewable transmitter, lighting up north and eastern Germany, as well as central and eastern Europe.

The firm is the core partner of the 2012 Clean Tech Media Award, a prominent green technology prize in Germany.

Prime targets

According to a McAfee report earlier this year, power grids are a "prime target" for cyber-attack because they depend on a myriad of embedded systems, all communicating with each other via a pot pourri of wired, wireless, cellular and dial-up modems, that use a combination of TCP/IP and proprietary protocols.

"This has expanded the attack surface, making it vulnerable to cyber threats," the report says. "Open systems invite hacking."

"The more automation there is in the grid - and we are currently fully automated - the higher the risk," Schucht said.

Some 70% of the existing energy grid is thought to be over 30 years old, another source of vulnerability.

Smart grids

If anything, the potential for disrupting more advanced 'smart' or 'super' systems in the future is thought to be even greater, because of the way that millions of interconnected nodes will link industrial and household smart meters with grid supplies.

"That something different as there are no smart systems connected to our system in Germany," Schucht said. "But this will change in the future," he added.

At least 80% of electricity users in the EU must be equipped with smart meters by 2020, because of the EU's internal market for electricity and gas directives.

This in turn should enable great cost savings for consumers – and energy savings for the planet – but the costs of securing the system may prove prohibitive in times of austerity.

Utilities would have to spend nine times more than at present to insure against a 'digital pearl harbour', according to a recent Bloomberg survey.

"We weren't aware of the risk five or ten years ago and we were investing in cables," Jacques Vandermeiren, the CEO of 50hertz's parent group Elia told EurActiv.

"But now cyber-security is one of the most important items on the agenda of all TSO's," he went on. "We spend a lot of money on hardware so it would be a shame if we were attacked through our software."

Table of Contents

China's Growing Military Might Obscures the Real Threat of Cyberwar

By Grant Brunner, ExtremeTech, 20 Dec 2012

China is growing in military prowess. Obviously, the manpower available is unmatched, but the technology is catching up as well. Their military budget has jumped to $100 billion in the last decade. It's only about a sixth of what the United States spends, but China is growing fast. In ten years, their budget has quintupled. China is eyeing its role as a military and economic superpower, and other countries should be concerned, but not for the obvious reasons.

A fantastic overview at Popular Science points out that the US only learned of China's J-20 fighter jet last year when Secretary of Defense Robert Gates visited the country. China is also ramping up production of unmanned aerial vehicles (UAVs). The Yilong rivals the American Predator drone, while the BZK-005 compares favorably to the Global Hawk. Even more interesting is that China has been working on retrofitting an aircraft

carrier of Soviet make and vintage. Liaoning, China's name for the recommissioned vessel, will sport surface-to-air missiles, an automated machine gun, and the capability to carry fifty aircraft.

While China's increasing might is reason for concern in the long term, it isn't nearly as worrisome as the work being done in cyberwarfare and satellite manipulation. At least for the foreseeable future, there is no way China is going to stage a worldwide coup against the United States and its allies. Its economy is intertwined with the United States, and damaging that relationship would undoubtedly send both economies into a tailspin. In reality, China's spying and satellite manipulation will do the US the most harm — not their fighter jets or drones.

Just last month, a report from the US Congress highlighted what a problem Chinese cyberwarfare has become. Cyber attacks account for about 15% of all internet traffic, and the vast majority of that comes from China's People's Liberation Army (PLA). China continues to attempt to interfere with US satellite communication, and has even been successful numerous times with at least two different US government satellites. Even scarier, they are dedicating resources to physically harming satellites in space. Not only do they have missiles that will take them out, but the PLA is also developing laser systems to effectively blind other satellites. They're even making microsatellites that can be used to ram into other spacecraft to either destroy or knock them out of orbit.

Conflict with China will not be conventional or even openly hostile, it will consist of fighting over data and technology instead of land or political ideals. While the US and China smile and work together publicly, they are entrenched in a deep and sophisticated cyberwar, and it's only going to grow from here on out.

Table of Contents

US Official: North Korea Likely Deceived US, Allies Before Launching Rocket

By Barbara Starr, CNN Wire, 27 Dec 2012

North Korea likely engaged in a deliberate campaign of deception before a December 12 long-range missile launch, catching the United States and its Asian allies "off guard," according to a U.S. official with direct knowledge of analysis of the incident conducted by U.S. military and intelligence agencies.

The official told CNN that American and Japanese military ships and missile defenses were fully operational and protecting land, sea and airspace on December 12, but that the launch was a surprise when it actually happened.

"We had our dukes up, operationally, but we were caught off guard," the official said.

"The clues point to a concerted effort to deceive us," the official said. The analysis was ordered in the wake of the launch to determine what exactly happened and how much the U.S. intelligence knew at the time.

The official said one conclusion was that while missile defenses can fully protect against a North Korean attack, the North Koreans have shown they can counter U.S. measures to gather intelligence about what they are up to.

"Look, they know when our satellites are passing overhead," the official said. It's believed the North Koreans essentially manipulated the launch so U.S. intelligence satellites simply would not be overhead and able to see what was happening.

The most likely scenario, the official said, was that North Korea wasn't telling the truth when it announced several days before the launch that there were technical problems with the missile.

According to the official, the intelligence analysis found that:

-- The United States observed the North Koreans beginning to take apart the three-stage rocket and move parts of it away from the launch pad, then observed what were believed to be so-called replacement parts being moved in.

-- In retrospect, those parts appear to have been from a second, older-generation long-range missile that were in storage. Those parts most likely were never used in the December 12 launch.

During this time, when the United States did not have total visibility of the launch site, it's believed the North Koreans either quickly reassembled the original rocket and fired it.

-- It's also possible the U.S. miscalculated and the North Koreans never took it apart at all.

Earlier this week, South Korean defense officials warned that the latest North Korean missile had the capability to travel more than 6,000 miles, meaning this type of rocket could strike the United States. However, experts do not believe Pyongyang has a nuclear warhead small enough to fly on the kind of missile.

North Korean officials claimed that the rocket launch succeeded in putting a satellite in orbit.

Table of Contents

Cyber's Next Chapter: Penetrating Sealed Networks

By Zachary Fryer-Biggs, DefenseNews, Dec. 16, 2012

Not long ago, if your computer network was cut off from the Internet, devoid of wireless routers and hunkered behind locked doors, you were safe.

But not anymore.

Several U.S. industry and military labs are improving the deciphering of the 1s and 0s that traverse these carefully guarded networks, and finding ways to inject data and infect systems with destructive viruses — "jumping the gap" into an ironclad network.

The progress in adding information to a network begins a new chapter in cyberwarfare, and the U.S. Army is looking to test the scientists' handiwork. This new chapter also shows how longstanding research on the physical science of electromagnetic fields and radio frequencies is coming into play in the realm of cyberwarfare, an area typically focused on software.

The Army's Intelligence and Information Warfare Directorate (I2WD) hosted a classified planning day Nov. 28. Sixty entities attended to discuss what can be done in the realm of electronic warfare and cyber, according to a source familiar with the program.

The roughly half-dozen objectives of the Tactical Electromagnetic Cyber Warfare Demonstrator program are classified, but the source said the program is designed to demonstrate ready-made boxes that can perform a variety of tasks, including inserting and extracting data from sealed, wired networks.

Being able to jump the gap provides all kinds of opportunities, since an operator doesn't need to compromise the physical security of a facility to reach networks not connected to the Internet. Proximity remains an issue, experts said, but if a vehicle can be brought within range of a network, both insertion and eavesdropping are possible.

The Army program is designed specifically to test capabilities for air and ground platforms, according to an invitation to an information day on the program released by I2WD. The invitation does not provide details on the specific targets for the program, instead including several buzzwords and encouraging attendance.

The program, which will consist of a series of demonstrations roughly every three months for the next two years, will test a variety of electronic warfare (EW) capabilities, said Moses Mingle, branch chief of the EW systems ground branch at I2WD.

"It's not a system, it's a demonstration platform," Mingle said. "Basically, we're vetting systems concepts, tactical EW cyber scenarios that could be deployed in the future."

Asked if one of the objectives is to demonstrate a system that could jump the gap and access systems remotely, Mingle declined to go into detail, citing classification issues, but said, "That's a part of it, but not all of it."

The source said the other objectives were more typical fare, including counter-improvised explosive device efforts. But the convergence of cyber capabilities and EW in the form of a box that provides easy access to a sealed network is likely the most sensitive aspect, given the questions surrounding the legality of certain cyber attacks and continued secrecy in the area, the source said.

Detecting Signals

Concerns about outsiders eavesdropping aren't new, as various intelligence agencies became increasingly worried in the 1980s with what are called compromising emanations, the electromagnetic field distortions that give away electronic activity. The study of the emanations was code-named TEMPEST, and led to a variety of efforts to shield systems. Researchers found that keystrokes could be detected from signals sent from keyboards to computer units, as well as information on a monitor.

And while the detection of these disturbances has become increasingly sophisticated, with systems able to pick out signals from greater distances with greater clarity, advances in the insertion of data using radio frequencies are gaining special attention.

The ability to add data still has limitations, mainly proximity and bandwidth, experts said. At current levels, complex data can take extended periods to insert.

Experts declined to provide full specifics on data transfer rates and range, citing the classified status of the capabilities and national security issues. But the possibilities are being explored as the U.S. military increasingly recognizes the potential of cyber weapons in operations.

The actual technology that allows for the insertion of data isn't novel, said retired Air Force Maj. Gen. Dale Meyerrose, former associate director of national intelligence.

"This is old technology," he said. "The technology itself isn't new, but the application of the technology is new, and the software running the technology on some of these devices is new."

Meyerrose, who runs the Meyerrose Group, said connecting to closed networks using radio frequencies is about five years old, but some of the complications of cyber, including legal authority, have slowed progress.

"This could be used to drop a Trojan into a system," he said. "Like everything else in cyber, there are not a lot of legal parameters. Like everything else in cyber, our legal system is about 20 years behind."

The recognition that electronic warfare methods can be critical for future cyber application is clearly making its way up the leadership chain. Senior Pentagon officials are increasingly emphasizing the need for the U.S. to control the electromagnetic spectrum in the future, without going into specifics.

At a recent event at the Naval Surface Warfare Center's Crane Division in Crane, Ind., Adm. Jon Greenert, chief of naval operations, made the case.

"We have to understand better the electromagnetic spectrum," he said. "Cyber, our radar and communication, everything. If you control the electromagnetic spectrum, you control the fight.

Table of Contents

North Korea Steps Up Jamming

By Joon Ho Kim, Radio Free Asia, 2012-12-19

North Korean authorities have intensified their jamming of foreign radio broadcasts since the beginning of December, blocking signals from South Korea and the United States almost every day during the last month of a year-long period of mourning for the country's former leader Kim Jong Il, sources in China say.

North Korean jamming is usually sporadic due to electricity outages and the cost of special facilities, but has now been continuous since Dec. 1, said a source in the border city of Dandong, in China's Liaoning province.

"Listening to RFA [Radio Free Asia] and VOA [Voice of America] is almost impossible due to static, which has continued since the first of this month," the source said, speaking on condition of anonymity.

A source in the Yanbian Korean Autonomous Prefecture of China's Jilin province confirmed that static had disrupted reception of RFA broadcasts, adding that broadcasts of South Korea's KBS (Korean Broadcasting System) were also "getting harder to hear."

North Korean jamming signals have also interfered with Chinese broadcasts, leaving state-run CRI (China Radio International) programs hard to listen to, said another source, who recently moved to China from Sinuiju, in North Korea.

"[CRI] broadcasting used to have better sound quality than anything coming from South Korea, but they are now hard to hear because North Korea's National Security Department is sending jamming signals," he said.

Mourning period

Sources tied the unusual period of unbroken jamming to the first anniversary of the death of former North Korean leader Kim Jong Il, and said that the jamming will likely continue until the end of December.

Hundreds of thousands of North Korean soldiers and civilians gathered in Pyongyang on Dec. 17 for a mass memorial to the late dictator presided over by his son and successor Kim Jong Un.

But North Korea's mood of mourning was briefly broken last week by the launch of a long-range rocket that successfully placed a satellite in orbit.

North Korea's authoritarian leaders typically fear that foreign broadcasts will undermine official narratives of important events, possibly leading to the current period of intensified jamming.

Speaking from Beijing, one observer of North Korean affairs said that if foreign radio is now difficult to listen to in the border regions, it may be "impossible" for a time to hear in North Korea itself.

North Korean authorities usually find it difficult to block all broadcasts, though, he said.

"More than 10 radio stations broadcast into the country from South Korea, and other broadcasts come from the United States and Japan," the source said.

“They send signals on many different channels, so it is hard for the North Korean government to jam all radio broadcasting from outside the country.”

Table of Contents

Information Warfare: Cyber War Tools for the Infantry

From Strategy Page, 18 Dec 2012

December 18, 2012: The U.S. Department of Defense is asking American firms for help in developing better tools for quickly analyzing captured electronic data (cell phones, storage devices, and specialized military electronics). This is nothing new. For over five years the military has been using similar tools developed for police departments. For example, five years ago troops began taking a hacker analysis tool (COFEE, or Computer Online Forensic Evidence Extractor) with them on raids in Iraq. Microsoft developed COFEE for the police and military, followed by a similar tool that enables a non-hacker to analyze wireless network activity and determine which targets can be attacked with a variety of hacker tools and weapons. For nearly a decade DARPA (Defense Advanced Research Projects Agency) has been developing versions of this cyberattack system. Details don’t get released, as that would aid potential targets.

The navy and air force have been heavily involved with DARPA on these projects. This makes sense because both services have been developing similar tools for electronic warfare, particularly for aircraft. These systems tend to be largely automatic as pilots, or even weapons officers in the back seat of a fighter, don't have a lot of time to work a screen full of options. It's different with penetrating or disrupting Internet type wireless networks. These would be encountered by ground troops, both in combat or on patrol. The cyberattack system has to be simple enough for a soldier to learn how to use it with minimal (a few hours) instruction, but flexible and powerful enough for a more experience operator to get the most out of it.

These wireless analysis and hacking tools first showed up five years ago, about the same time Microsoft quietly introduced a powerful tool for getting past security on laptops and PCs running the Windows operations system (which about 90 percent do). The device was a USB thumb drive called COFEE. When you capture an enemy computer, you plug in COFEE and then use over a hundred software tools to quickly get whatever information is on the machine. COFEE can quickly reveal passwords, decrypt files, reveal recent Internet activity, and much more. A lot of this can be done without COFEE but with the Microsoft device, intelligence collection is a lot faster.

Microsoft distributed thousands of COFEE devices to police and military intelligence personnel in the United States and some foreign countries. COFEE was developed mainly to assist the investigation of Internet based crime. But military intelligence operators find it very useful in uncovering enemy plans quickly, so additional raids can be quickly made. Islamic terrorists love their laptops and never go killing without them. The success and popularity of COFEE got the ball rolling on similar tools for other aspects of Cyber War. COFEE has been upgraded several times since it first came out, in part to get around hacker tools developed to defeat COFEE.

Table of Contents

Unwitting Sensors: How DOD is Exploiting Social Media

By Aram Roston, DefenseNews, 13 Nov 2012

Consider a selection of tweets posted one day last month. Some were humorous, like those of Steven Colbert (@StephenAtHome) hawking his latest book: “For a free sample of my writing,” he quipped, “see this tweet.” Tiffany’s (@TiffanyAndCo) tweeted a costly tip: “Layer silver and gold pendants for an eclectic look.”

And supporters of Somalia’s al-Shabaab militant group used the Twitter handle @HSMPress to boast of three blasts in Mogadishu: “The third explosion occurred at the city’s former police station where the apostate militia were preparing to occupy.”

On any given day, 400 million short messages are typed or thumbed onto Twitter, and that’s just a fraction of the total communications sent through a social media universe that includes Facebook, Google+, chat rooms, bulletin boards and many other electronic forums. The messages are as diverse as all the conversations in the world, at least those parts where there are computers, smartphones and iPads. And the effort to extract important data points and patterns from this digital cacophony has become one of the biggest growth areas in intelligence.

“The face of ISR has changed,” says Joshua Hartman, a former senior Defense Department intelligence official who is CEO of Horizon Strategies Group. “Open-source and crowd-sourcing information is a critical component of ISR.”

The potential products of such tools are endless, and reach from the tactical and immediate to the strategic and global — not just to find out, say, who is "following" or retweeting the al-Shabaab postings, but to be able to query where anti-government sentiment may be clustered in Pakistan or what expat Iranians living in Dubai feel about the ayatollahs back home and at what time of day they feel that way. Is the riot in Cairo about food prices or about a video offensive to the prophet Mohammed?

Barry Costa, a senior program engineer at the federally funded MITRE Corp., recently coined the term "population-centric intelligence, surveillance and reconnaissance." It's gradually replacing another term MITRE came up with: "social radar."

Costa says it's not metaphor: "Sonar was invented back in the 1900s to let us see through the water. Radar was to see through the air. Infrared lets us see through the dark. And social radar or population-centric technologies let us see the human environment."

Along the way, though, there is some unease, in privacy rights groups and even social media proponents, about the intelligence community exploiting these rich new streams of data: They may be open source, but the public communications of American citizens are all swept into the wash, sifted through and monitored by the technology.

Anyone can sign up for Twitter and follow a dozen or a hundred or a thousand fellow tweeters, but for a comprehensive analysis of all 400 million daily messages, you need to pay. What Twitter Inc. calls "the full Twitter Firehose" is a specific product that includes everything except private messages, and what the company calls "protected" tweets. Gold to marketing and brand analysts, the Firehose contains a stew of confessions, tastes and passions, a directory of people and their links to each other and what they are thinking about at any moment.

Among the small group of companies that buys the Firehose is Attensity Corp., a Palo Alto, Calif., company that sucks in Twitter and many other social media and then markets a vast amount of data and analysis.

"We have a massive-scale social media feed," said Michelle de Haaff, Attensity's vice president of strategy and corporate development. "150 million sources across 32 languages, and we sell the feed along with the analytics. And we sell that to the government and to commercial entities."

Twitter's Firehose is one of the stars in the Attensity showcase. "We have a contract directly with Twitter," de Haaff said. "We get everything across every language. We are pulling the whole thing. We are able to sense, understand and find signals: sentiments, hot spots, trends, actions, intent."

In countries where people use Twitter, she said, the company culls rich information.

"In Libya," she said, "we were able to track everything: where the arms were, where the rebels were moving. We had on a map where everything was going."

Among Attensity's early and crucial investors was In-Q-Tel, the Central Intelligence Agency venture capital fund that backs technologies of potential use to intelligence agencies.

From the beginning, the CIA was not just an investor but also a customer.

"As part of their investment, the CIA gets the software. They get a license," de Haaff said. "I can confirm they are still a customer, but that's all I can do."

Most of Attensity's government sales are handled through a "reseller" called Inttensity, a social-media-analysis company based in Catonsville, Md. A paper on Inttensity's website underlines the company's "pre-negotiated access to the Twitter Firehose" and similar agreements "with social media aggregators for content to discussion boards, forums and blogs from around the world."

In 2010, Inttensity won a Defense Intelligence Agency contract to provide a combination of the Inxight ThingFinder and Attensity Server text-extraction systems. (Inxight is another analytical system funded by the CIA's investment arm.) That contract didn't mention social media.

But two years later, the State Department awarded a $142,000 contract to Inttensity for a "social media command center," according to the Federal Procurement Data System.

A source close to Inttensity said it's an effort "to better understand foreign populations and what they really think."

Last year, the company hosted a "federal social media summit" at the Pentagon City Ritz Carlton in Arlington, Va. Federal officials from various agencies packed the ballroom. One of the speakers was 30-year-old Dan Zarrella, a kind of social media scientist who had focused on commercial exploitation of the technology. He'd never realized the military and intelligence agencies were pursuing it as well.

"The thing that surprised me at the Inttensity conference is how much interest the federal government has and how far along they are in recognizing the power that's there," he said.

One of the efforts on this front has been driven by the Office of Naval Research, which doesn't just fund MITRE's social media research, but also coordinated a Lockheed Martin program to predict crises using traditional open-source media. An official from the office was a keynote speaker at the Inttensity event.

A Pentagon spokeswoman, U.S. Air Force Lt. Col. Melinda Morgan, declined an interview but emailed a response to questions about population-centric ISR. She said traditional ISR could detect a crowd's activities but not a crowd's intent.

"Population-centric ISR consists of technologies and techniques that allow us to see and understand the human environment," she said. "Population ISR gives us a capability to determine narratives that drive behavior and allows us to more effectively communicate with audiences with whom we would engage. Population-centric ISR gives us a global and persistent indications and warnings capability that complements and enhances conventional sensors."

At the GEOINT 2012 Symposium in Orlando, Fla., in October, several of the exhibitors were hawking social-media analytic products.

Among the companies was Aptima, which developed E-Meme software under a $750,000 contract with ONR's Human Social, Cultural and Behavior Modeling Program. E-Meme stands for "Epidemiological Modeling of the Evolution of Messages," and Aptima says it tracks the spread of ideas on the Internet in various countries. There's an intriguing twist: "We are using the metaphor of it spreading like a disease," explained Robert McCormack, associate director of Aptima's analytics, modeling and simulation division. "We are looking at dynamics of transmission of ideas. For it to spread from person to person, you have to have some kind of contact between the people. And then you have to actually transmit the disease. Same thing here: The idea has to be transmitted."

McCormack said the company doesn't use Twitter at this point, just blogs and news sites. And he said it's all still in the development stage.

Another company hoping to become a player in this realm is Booz Allen Hamilton, whose website claims the firm offers "the most powerful and sophisticated tools for extracting value from Social Data."

At GEOINT, a program manager who asked that his name not be used showed off OSIRIS, one of the company's social-media analysis programs, to display tweets published over the last 24 hours in Syria. "I look right here," he said, using the mouse to move his cursor, "and we see a large spike take place. I can drill down into it and actually see the individual Twitter messages that took place."

One tweet on the screen says "Smoke rising." Another, heavily retweeted, message says, "three families have been wiped out in Hama, 54 people killed."

Susan Kalweit, a principal in Booz Allen's geospatial business, said the Twitter Firehose — which her company accesses via contract with DataSift, one of the big warehousers of this type of data in the commercial world — presents unique challenges. Much of Twitter's content isn't thumbed in by people, but generated by machines. And while U.S. tweets contain geographic location in their metadata, many foreign tweets don't.

Kalweit said OSIRIS compensates for the lack of geographic metadata with software that recognizes place names and other hints about location, then attaches a latitude and longitude to the message. "We've been using Metacarta," a geointelligence software system, "which we found is pretty good at getting definitely to the city level and often below the city level in some of these — not tourist — locations. So that's really helpful when people talk about the city or about neighborhoods."

Kalweit said social media presents new methods of obtaining intelligence from people who may see or comment on events in real time.

"I think that there is a construct of [the] human being as a sensor," she said. "Human beings now are ground sensors."

For all of its value to intelligence agencies, population-centric ISR raises privacy concerns. There is no "Firehose minus tweets from U.S. citizens." Public tweets, no less than Internet postings of all sorts, are caught in the wash and monitored.

MITRE's Costa points out that this is all public data that people posted to open forums. "We take active steps to ensure the privacy of the data. We buy publicly available data from public sellers," he said. "When you look at Twitter, it is not one tweet that you care about; it is about 100 million tweets. It's very rare you get to the individual Twitter level."

Tweets, except the ones users have marked as private, are open for all to see. Indeed, the Library of Congress has said it plans to archive all public tweets for historians.

CIA spokesman Todd Ebitz emailed that "The CIA focuses exclusively on the collection of foreign intelligence. In fulfilling this mission, the agency is vigilant about the protection of American citizens' civil liberties and privacy rights."

And the Pentagon's Morgan emailed that "all research is conducted strictly within the privacy guidelines set by law and DoD policies." She added that the focus of population-centric ISR is overseas and that the programs "are designed to support Combatant Commanders with areas of operation outside the U.S."

But even if each tweet and bulletin board posting is for public consumption, no more private then a scrawled message on a bathroom wall or graffiti on a bridge, there is unease about systematic government monitoring.

Rainey Reitman of the Electronic Frontier Foundation said that technically, it is indeed all legal, but she emphasized that people don't really understand how their random thoughts, disclosures or opinions on social media may be exploited.

"I think people don't realize when they sign up for these sites that the government is going to be routinely monitoring and sifting through this data," she said.

"If Coca-Cola is reading all my tweets," Dan Zarrella points out, "it's not as scary as if the DOD is reading all my tweets, right?"

Table of Contents

The Effectiveness of US Military Information Operations In Afghanistan 2001-2010: Why RAND Missed The Point

Paper by Major General (rtd) Andrew Mackay, Commander Steve Tatham Ph.D Royal Navy, and Dr Lee Rowland, The Behavioural Dynamics Institute, postd by IO Sphere, 3 Dec 2012

EXECUTIVE SUMMARY

In May 2012 the RAND Corporation published a detailed study of the effectiveness of US Information Operations in Afghanistan between 2001-2010. The paper identified six key lessons that the US must learn from that experience and made five recommendations.

This paper finds much to agree with in RAND's findings, but much, too, with which it disagrees, particularly in RAND's recommendations. However, it is the view of this paper's authors that RAND has missed THE fundamental failing in not just US IO and MISO/PsyOps but wider ISAF efforts as well:

A naive and immature understanding of the very process of communication in non-compliant conflict environments and misplaced confidence, and over reliance, upon marketing and advertising principles.

This paper advocates that marketing and advertising must now be considered as an utterly failed model for IO and MISO/PsyOps, one which must now be discarded in favour of a behaviorally-led approach embracing proper, proven, social and behavioural science.

During World War 1 the allies flew aircraft made of Balsa wood and fired archaic weapons across No Man's Land. In 2012 the allies fly super-sonic stealth aircraft and deliver precision weapons from unmanned drones. In World War 1 the allies dropped MISO/PsyOps leaflets. In Afghanistan in 2012 ISAF drops MISO/PsyOps leaflets. Unlike any other current military capability MISO/PsyOps has not evolved any substantial concept during the past 90 years. This paper, set against the backdrop of RAND's study, attempts to bridge that 90 year gap and in doing so identify the real reasons behind the failure of US (and wider ISAF) IO and MISO/PsyOPs in Afghanistan.

BACKGROUND

1. In May 2012 the RAND Corporation published 'US Military Information Operations In Afghanistan: Effectiveness of Psychological Operations 2001-2010', a report commissioned by the United States Marine Corps. This paper's single most important conclusion was that: "*if the overall Information Operation (IO) mission in Afghanistan is defined as convincing most residents of contested areas to side decisively with the Afghan government and its foreign allies against the Taliban insurgency, this has not been achieved*[1]". In assessing why this may be the case the report's author, Arturo Munoz, identifies six key lessons. These are:

- Inability to effectively counter Taliban propaganda.
- Inadequate coordination between IO and Psychological Operations (PsyOps)
- Long response times in approvals process
- Lack of IO and PsyOps integration in operational planning
- Absence of Measures of Effect (MOE)

- Poor Target Audience Analysis (TAA)

2. The report makes a series of five recommendations to improve the effectiveness of future IO and PsyOps activities. These are:

- Hold a conference of IO and PsyOps personnel who have served in Afghanistan to define best practice
- Use local focus groups to pre-test messages
- Conduct public opinion surveys for TAA and post-testing
- Use key communicators to help develop and disseminate messages
- Harmonise IO doctrine and practice and integrate greater integration between PsyOps and Public Affairs

3. In January 2012 this paper's authors published Behavioural Conflict: Why Understanding People's Motivations Will Prove Decisive in Future Conflict. All three authors welcome the detailed study undertaken by RAND and agree with the author's six key take away lessons, although not the recommendations. However, it is our view that the normally sure-footed RAND Corporation has, on this occasion missed fundamental errors in the US (and indeed wider International Security Assistance Force [ISAF]) IO campaign; further, we are of the view that the lessons they have identified simply do not articulate the problem either in breadth or depth. We find the recommendations anodyne, if not naïve; and by some margin distant from the more drastic action that we believe is now required by the West's IO and PsyOps communities if the errors of the past are not to be repeated in future conflict.

NOMENCLATURE

4. The 'tyranny of terminology' bedevils and inhibits nuanced understanding of these issues; indeed RAND acknowledge that IO and PsyOps have become almost indistinguishable in their usage. For the purposes of this document we define the terminology we use thus:

THE HISTORIC ELEPHANT IN THE ROOM

5. In 1916 the British Royal Flying Corps (the precursor to the Royal Air Force) flew Sopwith Pup fighters over the Western Front; a wooden bi-plane with a top speed of 106mph. Today, the Royal Air Force flies the Tornado, a super-sonic jet with a top speed of over 1200mph; In 1916 the Lewis Machine Gun fired 400 rounds per minute out to a range of 300m. Today, the British Army fires 700 rounds per minute out to a range of 2000m from the L1A1. In 1916 the allies dropped attitudinal PsyOps leaflets over the western front; in 2012 the US-led ISAF coalition drops attitudinal leaflets over Afghanistan.

6. Unlike any other current military capability PsyOps has not evolved in any substantial way during the past 90 years, despite the concept of 'influence' being now firmly embedded in western military doctrine, the psychological dimension of operations being regarded as central to success in Afghanistan and despite the science of behavioural change (and our ability to capture and measure it) having advanced rapidly and significantly over the last 60 years.

7. It is therefore our view that if there is one single reason why the International Security & Assistance Force (ISAF) have been unsuccessful in convincing Afghans in contested areas, we believe it to be a corporate failure to adapt IO and PsyOps' operating practices to the 21st century, instead relying upon ages-old methods of communication now proven moribund. If there is one single area more than any other in which this is obvious, it is in the over reliance of IO and PsyOps on commercial advertising and marketing strategies – substituting NATO and the Government of the Islamic Republic of Afghanistan (GIRoA) for the 'product' and Afghans for the 'consumer'.

THREE TYPES OF COMMUNICATION

8. There are three types of communication: Informational, Attitudinal and Behavioural. Understanding each is seminal to understanding why ISAF have been so unsuccessful in their operations in Afghanistan.

- INFORMATIONAL COMMUNICATION

As the name suggests, Informational Communication conveys from a source to an audience a piece of information that may not previously be known. In the context of military operations in Afghanistan, Informational Communication is regularly deployed. For example, ISAF may wish to explain why a Forward Operational Base (FOB) is being expanded or reduced; why military vehicles should not be tailgated, of new schools or community projects being undertaken in the area or of the number of the confidential Tip Line to report insurgent activities. All are perfectly valid and fall within the NATO definition of PsyOps: 'truthful and attributable activity directed at an approved target audience'. A good example of an informational poster is that shown to the left, informing the local population that a British serviceman was missing and what he would look like.

The audience's attention is also brought to the 110 Confidential Tip Line. Clearly this poster is designed to encourage behaviour (to find the missing serviceman), but at its heart it is informational, not least as the area in which the soldier was missing was immediately flooded with ISAF troops and the local populace would have been puzzled, perhaps even concerned, at their presence. Informational communication is a vital component in a counter-insurgency (COIN) environment; the insurgent will take every opportunity to twist events to their advantage. The insurgent typically is unbothered by either accuracy or veracity of message and, as important as being first with the truth is the need to constantly keep the contested population abreast of current events.

- ATTITUDINAL COMMUNICATION

This type of communication seeks to either reinforce positive attitudes or dislodge negative attitudes in discreet target audiences. In NATO's mission to Afghanistan it is perhaps best exemplified by the twin and long-standing projects of roadside billboards and newspapers. Across Afghanistan there are some 296 billboards which are used to promote GIRoA and 'good' governance. Concurrently ISAF produces a newspaper entitled Sada-e Azadi[2] which, in three languages, presents to literate Afghans a post-insurgency view of their country.

An example of an attitudinal type PsyOps product is shown here. In many areas of Afghanistan this is a message that resonates with Afghans, but that is not uniform across the country. As already noted, in many places the Afghan National Security Forces (ANSF) are simply not respected or trusted. Regardless, an Afghan's attitude to the ANSF may be swayed by this poster and it may give them confidence, but both of these are highly temporal, given to change rapidly if personal experience of deeds does not match the words.

- BEHAVIOURAL COMMUNICATION

This type of communication is focused on mitigating or encouraging specific pre-determined behaviours. For example, a PsyOps campaign may be used to directly target the trafficking of drugs, or to boost retention amongst the Afghan National Army.

9. The *poor understanding of each of these and their inter-relationships is, we believe, at the root of ISAF's IO & PsyOps / MISO failure*. Specifically we believe that it is remiss that behavioural communication is not employed more widely. Naively and unquestioningly implementing attitudinal campaigns are costly, particularly if the impact or effect sought – behavioural change – is highly unlikely. In any conflict environment it is the behaviours of different groups that determine outcomes, yet ISAF have pursued attitudinal change at the cost of behavioural change. It is rare, for instance, to hear senior officers talk of behaviours but exceptionally common to hear discussion of perceptions. For example, something as seemingly measurable as 'support for ISAF' must manifest itself ultimately in behavioural terms. How can we possibly know there is not support for ISAF troops if we were not observing specific types (or absence) of behaviours. It would be meagre satisfaction if opinion polls indicated that support for ISAF was buoyant, and yet there was no evidence of that support on the ground. Taking a behavioural approach to communication will lead the way to identifying which behaviours are most indicative of 'support', and what we can do to encourage them.

10. Behavioural communication can be surprisingly effective in changing some attitudes when an attitudinal approach is too obvious, or is unlikely to work. This stratagem was utilised to great effect during, for example, President Barack Obama's 'Change' campaign. Working closely with behavioural psychologists, the campaign team generated a social media 'viral' that aimed to excite people into turning up at Obama's rallies by informing locals that record numbers of supporters were to turn up, and it would be an incredible spectacle to behold. The idea behind this approach was that the very act of attending the rallies – even for non-Obama supporters and fence-sitters – would be so emotionally arousing and stimulating that people would form fresh positive attitudes towards Obama, and subsequently vote for him; history books bear testament to the idea's validity.

11. Because the attitudinal/behavioural issue is so poorly understood, and missed completely by the RAND report, we deliberately labour the point in this paper.

THE FOLLY OF ATTITUDINAL COMMUNICATION

12. In compliant societies attitudinal communication, which is the basis for commercial advertising and marketing, is largely used to differentiate between competing product brands. One brand of toothpaste, for example, is not significantly different to another, but if you associate with it, through an attitudinal marketing campaign, certain 'desirable' qualities or characteristics (for example, extra whitening capability, pleasant breath qualities etc) you effectively differentiate it from your competitors in the eyes of the consumer who is now more likely to purchase your brand. As a consumer walking into a supermarket you will be confronted by

an array of different toothpastes and your decision to purchase may well be swayed by an advert you have seen for a particular brand. The key to this, however, is that you have already made the decision to purchase; your behaviour has been predetermined by your upbringing (always clean your teeth before bed), your education (not cleaning your teeth will cause you painful medical problems) and other social factors (guys with bad breath don't get girls!) for example.

13. A further compounding problem is that there is much dispute amongst psychologists over what attitudes are, although what they are not is often easier to understand: they are not values or beliefs, and not really opinions, which are often terms used interchangeably with attitudes. In practical terms this means that attitudes are very difficult, in fact all but impossible, to measure accurately as they are influenced by so many other compounding variables. We collectively blanche when we see surveys that ask if an individual is 'slightly happier, much happier or considerably happier' with a particular issue; how can these possibly be delineated, so that trends across sample groups are measured?

14. However, the single biggest problem with the use of attitudes in PsyOps is that they bear so little resemblance to behaviour and ultimately, as we have already asserted, in conflict-ridden societies it is undesirable behaviour that the military must mitigate. There are numerous studies that show this to be the case. The first major study of its kind, and oft-quoted, is that conducted by Richard LaPiere in 1930s America. In his Attitudes Versus Actions study of 1934, which appeared in the journal Social Forces, LaPiere spent two years travelling across the USA by car with a couple of Chinese ethnicity. During that time they visited 251 hotels and restaurants and were turned away only once. At the conclusion of their travels LaPiere posted a survey to everyone of the businesses they had visited with the question, "Will you accept members of the Chinese race in your establishment?" The available responses were "Yes", "No", and "Depends upon the circumstances". Of the 128 that responded 92 per cent answered "No". This study was seminal in establishing the gap between attitudes and behaviours.

15. Because the West is a society where advertising is the norm, we accept, largely without comment, the deluge of adverts and marketing that we encounter on a daily basis. Indeed, it was because of this that the US expressed such astonishment when Al-Qaeda (AQ) seemed better at communicating its message than Washington: "How can a man in a cave out-communicate the world's leading communications society?", Richard Holbrooke famously enquired.[3] The answer of course is that Afghanistan is not a compliant society, where GIRoA / ISAF-friendly behaviour is the norm; indeed far from it. As we see from LaPiere's work the link between attitudes and behaviour is poor. Thus the problem with attitudinal communication is that it (erroneously) presumes that by changing attitudes, behaviours will follow (and clearly the behaviours that ISAF seeks in Afghanistan are in not supporting the Taliban, not laying IEDs, supporting GIRoA etc). The difficulty with this presumption is that firstly, Afghanistan is not a compliant audience waiting to be steered in a particular direction like the metaphorical toothpaste consumer of earlier, nor do NATO PsyOps necessarily reflect what is actually happening on the ground. The example below illustrates the point:

16. This ISAF road-side billboard, which extols the virtue and loyalty of the Afghan National Security Forces, is clearly designed to inspire confidence amongst those who see it. This is all well and good in a compliant society, one in which the rule of law is the norm. Yet in a society where corruption is endemic, where successful passage through a check-point will almost certainly require the giving of some money, such attitudinal communication does not stack up against the pragmatic reality of life on the ground.

17. LaPiere's work was closely followed by that of Fishbein and Azjen in 1947,[4] and has continued to this day as a vibrant area of scientific enquiry. The unequivocal consensus is that attitudes are very poor predictors of behaviour; indeed, one very influential social psychology text proclaims that: "The original thesis that attitudes determine actions was countered in the 1960s by the antithesis that attitudes determine virtually nothing."[5] For the non-social scientists amongst us a simple consideration of many circumstances in our own lives will lead us to the same conclusions. Some examples are illustrative:

• Car Seatbelts. For many years governments have sought to persuade drivers of the positive benefits of wearing a seat belt when in the car. They largely failed and it took enforcement (punishable by a fine) to make the wearing of seat belts an accepted and unconscious activity. Today, particularly if you are North European, we would guarantee that you put on a seat belt as an unconscious act as soon as you get into a car and will point out, often disapprovingly, if you see someone not wearing one.

• Cigarette Smoking. For years the UK government has sought to persuade the British public that they should not smoke. They did so with pictures of diseased lungs and warnings that smoking could curtail your life. Yet people continued to smoke and indeed in certain groups, notably young teenage women, smoking became more, not less, acceptable. However, one of the largest ever drops in smoking in the UK came about when, again, the government legislated and smoking in public places was banned. Apocalyptic tales of Britain's pubs and clubs going out of business were legion and landlords quickly put covered smoking areas outside their premises. Yet today people's attitudes appear to have softened and popping out for a quick cigarette in the cold or pouring rain is not quite such an attractive proposition as lighting up in warmth and comfort of a pub or bar.

18. Both these examples provide us with a second important lesson. Whilst attitude is a poor precursor to behaviour, behaviour is actually a very strong precursor to attitude. Or in other words, <u>if you change behaviour, even in non-complaint audiences, there is a good chance that with time that attitudes will follow suit.</u>

19. Because the West is so attuned and accepting of attitudinal communication it takes a real leap of faith to convince military commanders that adverts and marketing will not achieve the operational effect they seek. But we would venture that there is now enough evidence to dismiss advertising and marketing as a concept from the battlefield. This will of course be met with howls of protest form the civilian advertising community who have milked this particular cash cow since 9/11. Indeed in 2007, Todd Helmus, Christopher Paul and Russell Glenn produced a report, also published by RAND, entitled 'Enlisting Madison Avenue: The Marketing Approach to Earning Popular Support in Theaters of Operation'.[6] Their paper declared that "[b]usiness marketing practices provide a useful framework for improving US military efforts to shape attitudes and behaviours of local populations." In particular, the paper declared, attention should be paid to "branding, customer satisfaction and segmentation of audiences." We would venture that you do so at your peril. Take, for example, the segmentation of audiences. This is a standard marketing technique that looks to subdivide a specific sector of consumers – perhaps based on demographics or income or address - in the hope that the characteristics of this new group will be more susceptible to a marketing campaign. But this is very much a 'push' activity and the 'group' is an artificial construct that exists only on the marketers spreadsheet. Of course in military operations we are dealing with 'actual' groups, who are bonded by a myriad of factors outside of our control. It would be wonderful if, for example, our job could be done by targeting only the affluent, or the middle-aged, or women in a specific area. But in theatre, on operations, we do not have the luxury of choosing our own groups, we have to deal with the audience as it is in reality. Consequently, the process of Target Audience Analysis (TAA) is used to understand the actual group and to decode under what circumstances that group may be motivated to exhibit a specific behaviour. We are simply not interested in picking out a few 'potential customers' in the group, we need the whole group to conform (or at least a very, very,large part of it), otherwise we have failed in our mission. Commercial marketing and advertising methods are designed to increase the hit rate of customers in a target group. A conversion rate of 10% (i.e 1:10 buying a different brand of car or toothpaste) would be considered outstanding and highly profitable. But in military operations achieving a 10% change in the behavior of an insurgent group or a hostile community would be operationally insignificant. But perhaps most importantly, in the West, advertising is a well understood concept where there is an unwritten 'contract' between marketer and 'potential customer'. For example, we watch TV advertisements about Guinness or Ford – in the full knowledge that Guinness and Ford are trying to persuade us to buy more of their products. But this simply does not translate to the battlefield. **We have absolutely got to stop looking at audiences in foreign countries, often under-developed and crisis rich, through Western rose tinted lenses. We have got to stop exporting values and beliefs that we *do* understand to environments that we *do not*, in the hope that clarity will ensue. It will not.**

20. In Positioning: The Battle for your Mind[7], one of the most successful marketing books of all time, the authors, Ries and Trout, clearly make the point that marketing cannot change the way people think. It is behaviour we must study; behaviour we must understand; good behaviour we must encourage and bad behaviour we must mitigate. The solution is not branding and it is not customer satisfaction. And by implication the solution is not marketing and PR companies.

21. In marketing, the desired behaviour is fairly uniform, and quite identifiable: buy more of a product. The whole campaign, from planning to research to execution, wraps linearly around that single trajectory. Unlike the sorts of behaviours we seek to influence in Afghanistan, when selling products it is sufficient if just a small percentage of the target group actually buy your product. For instance, there are countless brands of toothpaste on the shelves, but if you get 10 per cent of the market, you can stay in business and make a healthy return to your investors. That is just not the case in many operational environments where it is vital that the majority of a group is influenced by PsyOps campaigns. Marketing is therefore not the kind of discipline that is equipped to deal with behavioural outcomes or scenarios that are more complex or require more nuanced definitions. Marketing principles just cannot be effective enough to drive our military capabilities and development; the end of that road can only be dramatic failure. In our view, only a scientific approach will do, and it must be based on the sciences pertaining to human behaviour, in all its myriad manifestations, and with all its bewildering complexities, and not the limited perspective of consumer behaviour, or the misguided assumptions of attitudinal psychology.

22. We think the tide may now be beginning to change. In February 2012 the newspaper USA Today ran an article entitled: 'US Info Ops Programmes dubious, costly'[8] in which it asserted that the Pentagon had spent hundreds of millions of dollars on poorly tracked marketing campaigns with little proof that the programmes worked. The paper quoted Colonel Paul Yingling who served three tours in Iraq between 2003 and 2009: "Doing posters, fliers or radio ads. These things are unserious". The same paper suggested in May 2012 that the Pentagon would soon be making yet further cuts to what it referred to as its 'propaganda budget'.[9] Yingling's comment "unserious" is absolutely right and that if the USMC wishes to understand why its PsyOps activities have been unsuccessful in Afghanistan then they need to look further than RAND's report.

BEHAVIOURAL COMMUNICATION – THE 'HOLY GRAIL' OF PSYOPS?

23. Behavioural communication seeks to link together specific communication activities to affect or mitigate audience behaviour. In assessing behavioural communication it is vital to take out the attitudinal dimension because it is largely irrelevant to the desired outcome. For example, if ISAF wish to deter Afghans from making Improvised Explosive Devices (IED), a behavioural campaign would study the motivations for making them in the first place. Almost certainly that analysis would determine that for some there is an ideological imperative that may be almost impossible to ameliorate or mitigate. Yet for many more there will be numerous other reasons for their actions. If we can understand what those motivations are, both amongst the current community that practice the art and those that might replace them in the future, then we can intervene effectively.

24. To adopt and apply a behavioural approach to communication requires a scientifically accurate understanding of human behaviour in real environments. Perhaps the most important principle to acknowledge is that the enacting of behaviours is always contextual. That means that people's behaviour is continually modified by the context in which it is played out. Factors such as environment, mood, social situation, and physical ability will determine whether and how a behavioural disposition is displayed. Some examples from Afghanistan will make this clear.

- Environment. The environment in Afghanistan is, in most places, harsh, and will have an effect on behaviours in numerous ways. Consider that in the worst months temperatures can reach 50° centigrade - anyone who has been to a very hot country will know how hard it is to motivate oneself to do anything under such conditions. Also, the environment will affect activities such as agriculture, such that even if a farmer is willing to plant an alternative crop, he may simply not be able to do so.

- Mood. Some areas of Afghanistan and some strata of Afghan society suffer from persistent drug problems. In areas where this is severe, decision-making and motivation will be significantly compromised. Emotional states can be profound and enduring too amongst Afghans: loss of honour amongst men will be all-consuming and will not be rationalised. These feelings will persist until avenged.

- Social situation. Respect for elders is paramount, and decisions are often made collectively, with the senior members holding sway. Individual preferences are subjugated to those of the group, for instance, in voting. A strong social network is most prized, whereas wisdom holds little weight. It is a case of 'who you know, not what you know' in Afghanistan. One aspect that is often misunderstood by Western influencers is that individual achievement means little to Pashtuns. Achievement from the perspective of the village or community is the overarching goal.

- Physical ability. Afghans are limited in what they are capable of doing, often because they do not have the means or skills. Things like voting, watching television, travelling to large towns, reading papers or leaflets, using telephones to report insurgent activity, and a wealth of other activities can often be hampered because of physical limitations, and not necessarily attitudinal or emotional ones. If people cannot get to voting stations or recruiting stations for instance, then no amount of persuasion is going to help. This is where

behavioural influence offers a solution that supersedes communication or attitudinal approaches: the behavioural campaign would alter behaviours by providing the necessary means to carry out the behaviour. If you want people to vote, then make sure they can get to the voting station – or, better still, bring it to them. (Although, as an aside, there is evidence that voting behaviours can be influenced by the environment in which people place their vote. For instance, voting in a school assembly room can 'nudge' people to vote for the party that places most emphasis on education.)

In these four simple examples, we show instances of where behaviour is shaped by factors other than personalities, attitudes, desires, and tendencies.

25. In the 1920s Yale psychologists Hartshorne and May[10] investigated the extent to which character traits determined behaviours. They were interested in whether different situations would influence schoolchildren who were given the opportunity to lie, steal or cheat. Across 10,000 children they found that most of them behaved badly in some situations and not others. But perhaps most important is that these behaviours did not correlate with measurable personality traits or assessments of moral reasoning. In technical terms, this research (and much more like it) demonstrates that behaviour rarely displays 'cross-situational stability'.

26. In short, people's behaviour is controlled or modulated by a whole host of personal, social and environmental factors, many of which are beyond the control of the individual, or only marginally in his or her awareness. Any attempt to understand and change behaviour therefore needs to identify the causes present at all levels, and not simply focus in on the personal, or the social, for example. This approach is termed the ecological method for it seeks understanding in a broad context, at all levels and in a naturalistic way, i.e. what people actually do in their real lives.

27. Now, if we are willing to concede that our own behaviour is subject to all sorts of influences that are mostly beyond our control, are we not also able to extend that same understanding to Afghans? It is difficult enough in our own safe and predictable world to always behave as we would like, and in accord with our attitudes and opinions. Should we not therefore see the difficulties that the average Afghan faces, in a harsh social and physical environment, in a country ravaged by war and hardship? To expect that there should be any straightforward relationship between attitude and behaviour is farcical.

28. Consider Figure 3.13 on page 61 of the RAND monograph. It shows that the Afghans perceive the biggest threat/danger to be from the Taliban (approx. 60 per cent), with very little from the US (less than 10 per cent). This sounds like good news. But what does it really mean? Does it mean that they will behave in an agreeable manner towards coalition forces? Does it mean that they will reject the Taliban, or behave unfavourably towards them? Does it mean that they perceive the US positively? We do not think the result relates to any of these possibilities. Moreover, if Afghans regard the Taliban to be a greater threat, and yet their behaviour remains unaltered, then we are no closer to a solution. We need to understand what it would take to get the Afghans to reject the Taliban and embrace the ISAF's efforts. Just because the population do not think that the US is a threat, does not mean that they respect them (they could think they are just ineffective or too timid). The locals could quite reasonably believe that the US poses little threat to them, and still hate them with a passion. It is just this kind of attitudinal polling that is preventing progress in Afghanistan on the things that really matter, something we discuss below.

29. RAND's paper presents a brief evaluation of an anti-IED campaign that appeared to have a modicum of success in changing behaviour. We quote from page 78: "*In some places, there have been verifiable, positive results, with local people volunteering critical information. In other places, the locals remain too afraid of the Taliban to come forward. The key variable here seems to be not the credibility of the USMIL IO and PSYOP but the degree of fear of the Taliban and the credibility of the Taliban threat against collaborators."* This exemplifies the point we make. The campaign has looked at the target audience from an attitudinal perspective. As RAND note, it is not the credibility of the message campaign that is the key variable. Indeed, the campaign *may* have entirely succeeded in changing the attitudes of the local population, but crucially it has done very little to actually change behaviour. What use is it in providing information about how to report IEDs and in shifting a change in attitude in favour of doing so if there is no appreciable and measurable change in people actually providing information to our troops? Proper PSYOPS and IO initiatives need to begin by asking: under what circumstances would behaviour change? As we have already noted this is not audience segmentation.

HOW TO ACHIEVE BEHAVIOUR CHANGE

30. We have already explained that contextual factors are critical to the manner in which behaviours are (or are not) displayed. These need to be assessed and understood at the beginning of any behavioural campaign. However, once it has been determined which behaviour(s) you want to try and change, attention needs to turn to the question of *how* change can happen. This is a very complex question and area of study, and a full

answer goes well beyond the scope of this paper. Nevertheless we venture several principles drawn from the behavioural and social sciences.

31. A good starting point is the triumvirate of awareness-motivation-ability. These are the 'Big Three' of behaviour change, because without them being in place, widespread robust change cannot occur (except by force). Awareness often comes first because if your target group does not know about the behaviour you want them to enact, then it is highly unlikely that they will start doing it spontaneously. If you want to get young men to join the ANSF, then they at least need to be aware that recruitment is happening and where. Motivation follows because awareness will not change behaviour if there is no way to motivate the desired behaviour. It is almost impossible to get someone to do something if they don't want to do it, unless you use threats and force, or you make it worth their while. But lastly, even if your group is aware of what is required of them, and they are willing to comply, they will perform the behaviour if they are not capable or able to do so. For instance, if there is no way of travelling to the recruiting station, then they cannot join the ANSF.

32. This all sounds rather obvious – and indeed it is – but it is surprising how many behaviour change campaigns do not consider these three fundamental principles. In the IED example above, it seems that the target population had awareness of the details of the campaign, and presumably there was some motivation (and incentive) to provide information to coalition troops. But did the people have the ability to do so? And were they sufficiently motivated to do so? Given the threat of the Taliban, perhaps the motivation to stay on their good side was greater than to help our troops, even for a monetary reward. Perhaps the reporting channels were just too risky or too conspicuous? If there were an entirely non-risky and anonymous way to provide information (i.e. no way, ever, that the informant could be found out), then the 'ability' factor could have been enhanced.

33. Another fundamental consideration in building any behaviour change campaign is that of the power of social norms. Social norms are the socially accepted standards and codes of behaviour that most people in a group or society conform to. For example, in British society sexual discrimination has become socially unacceptable in the last few decades. This is quite independent of individual attitudes however. We can imagine that men still exist who privately think that women should not be paid as much at work, or who should not occupy high positions, but the likelihood of actually displaying that trait is now very low.

34. Elizabeth Levy-Paluk is a field social psychologist who trained at Harvard, and has done experimental work on the Hutu and Tutsi ethnic tensions in Rwanda.[11] In a year-long field study, she used specially crafted radio programmes to try and change attitudes, beliefs and norms of tribes in a bid to reduce inter-ethnic conflict. The study was carefully designed according to rigorous scientific standards, she used appropriate controls, and meticulously collected data through interviews and covert and overt behavioural observations. The study proved very effective in positively changing the behaviours of the two groups towards each other. Her conclusion drawn from the data was unequivocal: whilst the study did little to change the beliefs of the people, it was very effective at instilling social norms, and these social norms drove the observed measurable changes in behaviour.

35. RAND notes the research work conducted during September-October 2010 in Afghanistan by UK Strategic Communication Laboratories (SCL) which showed that ANP recruitment was powerfully influenced by binding social norms that deterred young men from joining up. Many potential recruits were motivationally and morally pre-disposed to work in the ANP. The desire for a job and reasonable pay was very high, and they desired to do good for their country and thought that by being a police officer they could make a difference. The research discovered that the main reason holding men back from joining was the fear of recrimination, hostility, or being ostracised by the wider social group, that is, the mothers, the elders, older men, and disapproving peers. The research further uncovered that the primary reason for the existence of those social norms was that the ANP were deemed to be un-Islamic. The research concluded – through the use of some complex statistical modelling of the data – that boosting the Islamic credentials of the ANP would be the most effective way of breaking down those social norms and consequently boosting recruitment.

36. Both Paluk and the SCL studies amply illustrate why the attitudinal approach will not work. The types of problems being dealt with in these environments with these populations are just too complex for a superficial marketing approach. In contrast, properly conducted scientific research based on a behavioural model can arrive at solid conclusions and achieve results.

37. Although having a nuanced understanding of your target group's contextual motivations for their behaviour and how social norms can modify behaviours, the problem remains of knowing *how and when* to intervene in effecting genuine change. If you are a frequent flyer, you may have experienced the annoying feeling of standing in the security queue and *only then* realising that you had intended (since your last flight) to not wear a belt, wear slip on shoes, have your toiletries already packed in a plastic bag, and to have your laptop at the top of your bag. But no, just like last time, you are ill prepared. By that stage, it is too late to

change your behaviour. You should have remembered all this back at home, but of course you were not thinking about it then.

38. Any airport wishing to speed up waiting times in security would achieve little if they placed reminders to be prepared at the airport, or worse, in the security queue itself. The decision point at which to reach flyers is when they are packing, or maybe as a reminder when booking their tickets. People who check in at home online could be reminded then, or perhaps provide a visible nudge on home-printed tickets. Knowing when best to reach people is as important as the message itself.

39. A recent UK Department of Transport campaign aimed to persuade young men not to drink and drive. The research pointed to a move away from shock tactics towards emphasising the negative personal consequences to the driver. Audience research, semiotics analysis and behavioural theory identified the key intervention point as being after the first pint when the subject is still in control and able to think straight. (The campaign was called 'Moment of Doubt', and used the word Think! in its adverts.) But obviously, the campaign could not intervene at that precise moment in time, so the proposed solution was to create *cognitive dissonance* that would hopefully kick in at the required intervention time. Loosely, cognitive dissonance is a psychological theory that proposes that inconsistencies in thoughts and behaviours will cause internal conflict. People often seek to reduce that conflict, either by changing their attitudes or behaviour so that they are more closely aligned. The 'Moment of Doubt' campaign therefore focused on the inconsistency between having another drink and the dire consequences of losing your license, getting a criminal record, and damaging relationships. The credibility of this argument and its manner of dissemination was clearly effective as although breathalysing increased in 2007, the number of people testing positive dropped by 19.5 per cent.

40. How do our troops go about determining the correct intervention points for Afghan campaigns? How do we decide which psychological theories are best suited to helping with message resonance? Knowing the ideal decision point for Afghan opium farmers, or the strategy for intervention on potential recruits are complex issues. It is hard to imagine how these kinds of strategies and results could come about without the deployment of good quality science informed by theories of behaviour change. It is imperative that these approaches are used in Afghanistan and that they are integrated into military practice for PsyOps, IO and similar disciplines as soon as we are able.

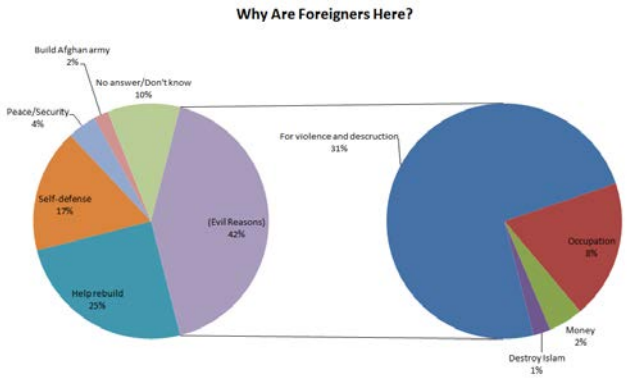
41. To achieve this level of success we need to base campaigns on better TAA and on better scientific theory, models and methods. All the knowledge exists, and, as we have seen, is being used to good effect in civilian campaigns. It is not possible in the context of this paper to provide extensive detail of the wealth of science that could be used. Besides, any decent social psychology textbook is a good place to start. But it will be necessary to bring in specialists and to tackle the arduous task of synthesizing and applying the knowledge of a vast number of disciplines to military communication. Social psychology we have mentioned, but we also need to bring in behavioural economics[12], system dynamics, environmental psychology computational behavioural modelling, group dynamics, and social network analysis, to name a few.

42. During a visit, by one of this paper's authors to ISAF, nine behaviourally-based IO and PsyOps campaigns were proposed. Two examples: 1) increase retention in ANSF and, in particular, the number of Pashtuns joining. Whilst the newspapers will often report that recruiting (from other ethnic groups) into the ANSF is buoyant, retention is less so. While the ANA is slowly becoming more broadly representative of the Afghan ethnic mix there remain notable gaps, for example the recruitment of southern Pashtuns. This cannot be good for the future. 2) Migrate men of fighting age away from the insurgency and into the sustainable livelihood programmes being run by Provincial Reconstruction Teams (PRTs). Yet all nine proposals were refused because they required upfront funding for qualitative and quantitative research and would have taken over 18 months to have come to fruition. Yet ISAF itself cannot undertake quantitative/qualitative research wearing body armour, carrying weapons and driving armoured cars – here there is a real need for contractor support which of course means money. But the ideas did not gain the necessary traction solely because of the funding issues alone, the reality is that no-one was really very interested in behavioural change campaigns that would outlive their particular tour in theatre. We find this absence of imagination and a slavish approach to process very concerning.

NARRATIVE

43. The Consortium for Strategic Communication,[13] an academic body located at the University of Arizona, recently published on their blog a report from November 2011 published by the International Council on Security and Development (ICOS). Professor Steve Corman, of the Consortium, wrote he had been 'floored' by the fact that when several ordinary Afghans had been handed pictures of the 9/11 World Trade Centre attacks almost none were able to identify the event or its location. Indeed the full ICOS report14 finds that only 8 per cent of those surveyed knew about the "event that foreigners call 9/11". A further question asked why foreigners were in Afghanistan. Of the 42 per cent who stated that they were here for "evil reasons", the

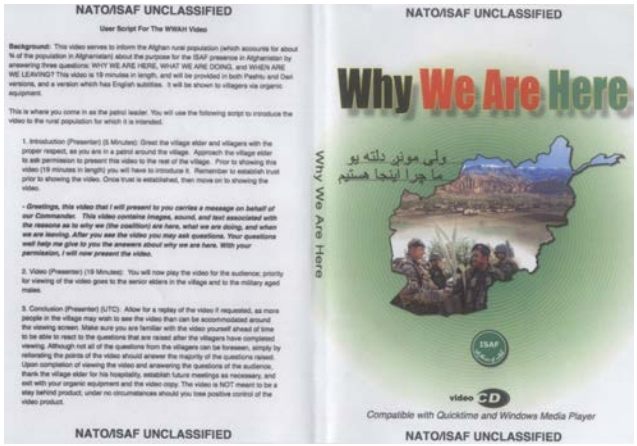
largest percentage believed it was for "violence and destruction". The graphic below details the other answers that were associated with the question:



44. The struggle to find a 'narrative' that resonates in the global information space has been one of the international community's most significant challenges, one that still has not been satisfactorily resolved. For the populations of NATO troop-contributing nations most ISAF members have adopted a similar framework: NATO troops are in Afghanistan to ensure that mass terrorism can never again emanate from Afghanistan and threaten European and North American homelands.

45. In the initial years after the 9/11 attacks this worked as a message, but over time, as memories of 9/11 fade, so too has acceptance of the message. Indeed events such as the 7/7 London bombings and the Madrid train bombs did not serve to reinforce a collective view of the righteousness of the Afghan mission, instead they have served to complicate the issue significantly. In the case of 7/7 the bombers were from the United Kingdom and the UK's continued presence in Afghanistan was given as a specific reason for the attack. And, as we have seen from the ICOS survey in paragraph 12 above, these are not motives that resonate with Afghans. In April 2010 the UK's now disbanded Advanced Research and Assessment Group (ARAG) secured funding from NATO HQ to bring some of the most experienced Afghan and communication scholars in the world together and work with NATO to produce a convincing narrative that would resonate, not just with domestic NATO audiences, but with Afghans. Some 10 years after the US-led invasion most Afghans were still unsure and unconvinced at the presence of foreign troops. Unfortunately, the explosion of the Icelandic volcano Eyjafjallajokull prevented the conference from happening.

46. In late 2011 ISAF issued a DVD to its troops on the ground entitled *Why we are here*. On its back cover it contains a script for troops on the ground to use: "This video contains images, sound and text associated with the reasons as to why we (the coalition) are here, what we are doing and when we are leaving". This latter point is of particular importance. In 2011 ISAF Headquarters, and the various Afghan governmental ministries, were already deeply engaged in the first stages of transition – the passage of responsibility for security away from NATO to the Afghan National Security Forces (ANSF). The issue of the DVD was a welcome, if very late, step forward by ISAF HQ who were beginning to understand that there existed a real understanding vacuum on the ground amongst Afghans who were not attracted to the Taliban insurgency, but who were equally unhappy at the presence of foreign 'invaders' in their country.



However, its timing (coinciding with transition and the gathering momentum to draw down forces in preparation for the 2014 withdrawal) presented very real problems to troops on the ground and in particular to NATO PsyOps practitioners who were struggling to explain, in local terms and in ways that resonated with their specific local audiences, what foreign troops were doing and trying to achieve.[15]

47. RAND's paper quotes Oleg Svet's 2010 assessment of IO in Afghanistan, which reviewed the roles of the State Department, Department of Defense (DoD), and the Central Intelligence Agency (CIA) in this area, concluding that *"[w]ith diffused authorities, it has been difficult to pursue a comprehensive narrative providing legitimacy for the local government, quickly respond to the Taliban's propaganda, and proactively shape the information environment."*[16] We would suggest that the absence of a convincing narrative has been a significant handicap in convincing Afghans of the presence of ISAF troops. We predict that this will be an issue of increasing concern; Afghans may not like the presence of international forces in their country but they have become accustomed to it, particularly as some areas have flourished and prospered. The transition to Afghan forces should be a comparatively simple and good news story to portray, but this is hindered by confusion over why ISAF is present at all and the capabilities of a still fledgling Afghan civil and civic society.

48. We must constantly remind ourselves however, that the average Afghan is not really interested in our 'narratives', even though we do still need one that is consistent. The RAND monograph quotes LeGree (2010):

When the IO campaign's radio spots, billboards, and public announcements exclusively focus on reporting improvised explosive device (IED) incidents, offer rewards for information about insurgents, or make clumsy attempts to paint the insurgents as bad guys, the audience is not interested. These things are simply not what the average Afghan cares about. It just gives the insurgents 'free press'. Tell a man how to grow more wheat on his small plot, give him access to a wider variety of food, or tell him about the bridge that will let him walk to a market and you have the audience's attention. These are the things that matter, the most effective subjects for the IO campaign.[17]

49. In keeping with our argument thus far, LeGree is close to offering a behavioural solution to the issue of communication: do not bombard the population with irrelevant (to them) messages conveying moribund ideas, give them something they can use, change their behaviour, get them doing something that might evolve into seeing the 'occupiers' and their Afghan sponsors in a favourable light. That is the most powerful form of communication imaginable, and we should be offering it.

50. The essential problem that ISAF faces when it considers the issue of narratives is that in western democracies the ruling political classes are under constant forensic scrutiny from their media and their electorates. Thus, narratives, which are inherently crafted by politicians, are almost always crafted for domestic audience consumption and the audience in the conflict zone is almost always forgotten.

MEASURES OF EFFECT

51. Quite rightly the RAND report identified the absence of robust and empirical measures of effect (MOE). Without MOE it is almost impossible to draw any sensible conclusions on the success, or otherwise, of IO and PSYOPS campaigns. Our experience is that if any thought is given to MOE then it is regularly in the context of measures of performance (MOP) or measures of activity (MOA). For example, the measure of activity associated with an airborne leaflet drop is that the necessary aircraft and equipment were serviceable and available to make a certain number of predetermined sorties. The measure of performance is that a specific number of leaflets or other products were dropped. The measures of activity are what specific actions the leaflets engendered in the audiences that they targeted.

52. Another attraction of behavioural, as opposed to attitudinal, campaigns is that MOE is all but impossible to measure in the latter. This is why surveys and polling blossomed so fully during the wars in Iraq. The focus has been on attitudes and survey and polling are a logical, if imperfect, way to measure changing attitudes. But in behavioural terms MOE is often observable. If the campaign is to grow less poppy you can visibly see if that campaign has been successful from the air. If the campaign is to encourage greater use of roads by private cars (and thus encourage a feeling of security) it is straightforward to measure road usage with a few strategically placed motion sensors. You could even measure accurately the numbers of calls to a hotline, and how many of those calls led to successful arrests or locating IEDs.

53. The key to successful MOE is twofold: Firstly, activity has to be properly baselined. It is no good attempting to measure behaviours, or for that matter attitude, after the IO/PSYOPS intervention if there is no record of what the behaviour or attitude was prior to it. RAND identify nine PsyOps campaigns in their report (below), noting whether they were effective, ineffective or not measurable.

Theme	Assessment		
	Effective	Mixed	Ineffective
The war on terror justifies U.S. intervention.			Ineffective
Coalition forces bring peace and progress.	Effective 2001–2005	Mixed 2006–2010	
Al-Qai'da and the Taliban are enemies of the Afghan people.		Mixed	
Monetary rewards are offered for the capture of al-Qai'da and Taliban leaders.			Ineffective
Monetary rewards are offered for turning in weapons.		Mixed	
Support of local Afghans is needed to eliminate IEDs.		Mixed	
U.S. forces have overwhelming technological superiority over the Taliban.	Effective 2001–2005	Mixed 2006–2010	
GIRoA and ANSF bring peace and progress.		Mixed	
Democracy benefits Afghanistan, and all Afghans need to participate in elections.	Effective 2001–2005	Mixed 2006–2010	

NOTE: IED = improvised explosive device. ANSF = Afghan National Security Forces.

54. From anecdotal experience and observation on the ground we actually think that the coalition PsyOps effort may have been more successful than RAND state, but they are right to question it as there is such a paucity of evidence. We would, for example, split the joint reference to the Taliban and Al-Qaeda. Whilst the former still enjoy significant support, the latter do not and we think that RAND could be more upbeat in their assessment. So too, the issue of the US having overwhelming military superiority. But the absence, until now, of a robust methodology for assessing MOE and the ever present paucity of baselines does not make the task easy.

55. It is rather worrying that RAND seem to vastly underestimate the complexity of conducting MOE in theatre. RAND notes that for PSYOPS to be effective the messages and means of communication must be credible. This, we would argue, is not so much a measure of effectiveness, but an aspect of communication that must be firmly established when conducting TAA. It is not clear from their presentation where they place the emphasis on this perception of effectiveness. Moreover, RAND's third criteria of effectiveness is that *"[o]perations must show evidence that audience perceptions or behaviour were influenced as intended*." We noted above that there is an alarming paucity of this 'evidence'. But equally, if not more, concerning is the lack of understanding of how hard it really is to do MOE properly.

There are several issues here.

a. **Establishing behavioural indicators**. From the outset it is necessary to identify appropriate behavioural indicators by which to measure change. This requires an in-depth understanding of the target group and their behavioural patterns, and a sufficiently rich awareness of which behaviours are most indicative of change. It is hard to do this in the beginning and actually must be based on high quality TAA of the prospective audience(s) to narrow down the possibilities. Often, several iterations may be needed to get this right.

b. **Causality versus causation**. The real devil in all this is how to unravel the competing effects of factors that *cause* the behaviour change and those that are merely *correlated* with change. A well-worn but classic example is that ice-cream sales increase in line with the numbers of drownings. This does not imply though that one caused the other. It is more likely that a third factor, hot weather, underlies both increases. How can we distinguish whether retention in the ANA has improved due to our behavioural campaign, or because more insurgents have infiltrated the ranks and wish to build up numbers for attacks from within? It is difficult to perform analyses of this kind, but if approached scientifically it is possible. Prominent US social psychologist Timothy Wilson has criticized the D.A.R.E anti-drug programme, which is used by 70 per cent of American schools, and yet, until recently, was not even tested. He explains on The Edge science website:

> *"If there's one thing social psychologists do know how to do, it's how to do experiments and how to test whether an intervention is working, and with good control groups and statistical analyses, seeing whether something works or not. Yet, a lot of the current programs in a wide variety of areas have never been vetted in that way, and are just based on common sense".*

The recent testing revealed a shocking result: the programme does not work, in fact it increases drug-use amongst the target population. MOE in Afghanistan needs to be based on rigorous scientific testing, not on weak *post hoc* or supplementary measures. MOE really needs to be woven into the process from start to finish. Granted, the RAND monograph (p. 28) does recognise the complexity of MOE and acknowledges the cause-effect hitch. We agree that it will not always be possible to relate cause to effect with certainty. Our concern however is that that should not deter us, and that we can do far better than we have currently done if

we (a) decide to do so, and (b) adopt proper scientific procedures (and employ scientists) to do the best job possible.

c. **Changes in audience**. Part of fulfilling the criteria above can be achieved by recognising that there are multiple stages of change (one influential behaviour model by Prochaska and DeClemete[18] is called the 'stages of change' model), and that these should and can be measured. By doing this we can get a more accurate description of how change is occurring and to what extent it relates to military actions. Between basic behavioural indicators and the kinds of large scale behaviour changes that campaigns seek to measure, many changes occur at the audience level that are more subtle, yet highly predictive of behavioural outcomes. These will include attitudes, intentions, motivational dispositions, and perceptions, and they need to be measured too. Not as an end in themselves, but as ways of gauging intermediate changes in target groups.

WEAK CORPORATE KNOWLEDGE

56. The absence of baselining underscores another failure of coalition PSYOPS and IO in Afghanistan that RAND does not mention – the educational deficit of senior military commanders. We do not mean this unkindly; what we mean is that front line commanders have been trained and exercised for years in kinetic effects. They are completely familiar with the type of kinetic effects that can be achieved, their risks, operating windows and likely benefits. Their mastery and application of that knowledge is why they are senior commanders entrusted with great military responsibility. Unfortunately the operating environment has now changed from that which defined their formative years. Today [mis]perception equals reality and one single individual with a camera-enabled mobile phone can cause seismic strategic unrest as, for example, the events of 23 August 2008 in Azizabad showed. The Pentagon was forced into an abrupt U-turn over its military strike when images of dead children emerged, taken on a mobile phone. Our collective experience of many senior military officers is that they fall broadly into two distinct camps: those that get 'it' ('it' being the power of behavioural influence campaigns) and those that do not. However, both are characterized by professional ignorance of what is achievable and what is not in this very specialist area. This points to a significant educational deficit; whilst western militaries are exceptionally well trained, education is always the poor relation and we think much more attention needs to be paid to the more unconventional aspects of current and future warfare.

57. It may be too late for Afghanistan but it is clear that countries such as China and Russia have developed very nuanced understanding of offensive IO techniques. To quote eminent scholar Dr David Betz of King's College London:

> *"Like the shock paddles of a defibrillator on the chest of a heart attack victim the prefix 'cyber' has an electrifying effect on policymakers and strategists wrestling with the complexities of information age security. Thus while in practically every other aspect of public expenditure the talk is all of 'austerity' there has been a bonanza of resources dedicated to countering the threat from the internet."*[19]

But not in other areas – like IO. Indeed quite the opposite, in the US and the UK IO capability is actually being reduced.

SURVEYS

58. The sheer number of polls and surveys undertaken in Afghanistan is astonishing, their results can be found all over the internet: from large polling organisations employed by ISAF through to indivisible national initiatives to measure their individual performance. But just how reliable is the science of surveys?

59. A significant determinant of the validity of polling is the manner in which the question is phrased and presented. But assuming this is done consistently across all polled groups, the reality of surveys is that they will only ever tell you what the polled thought about something at a particular point in time. Surveys and polling are highly temporal and closely related to attitudes. Far too much attention is paid to polling. For example, the Asia Foundation famously reported that 84 per cent of the Afghan population was happy with law and order in Afghanistan.[20] In a society with a rampant insurgency this was simply not a credible figure: it is unlikely you would get 84 per cent approval for policing in places such as New York City or London, let alone in a society in the midst of civil war. As one of our [very senior] proof readers privately observed:

> *"The Afghans appear to the most surveyed people on earth. Everywhere I turned when I was there in October 2012 another group was telling me how they had a poll… when I asked the MISO Task force how they controlled for over polling in their 200+ question survey, they told me with a straight face they had questions in the poll to control for that".*

60. By way of an example consider the recent US Presidential election and this front page headline reporting a GALLUP poll just days before the election. Polls and surveys cannot in the future be THE principle determinate of IO policy in the

way in which they have figured in Afghanistan. In their place we must use the tried and tested mechanisms of TAA.

COMMAND AND CONTROL (C2)

61. In ISAF Headquarters there are some 500 officers from all troop contributing nations planning operations and policy. In the IJC some 900 officers fill similar functions; at regional commands a similar plethora of officers plan. At the operational Headquarters a smaller but still sizable number of military staff plan. In our book *Behavioural Conflict* we opine that the defining sound of 21st century conflict is now the steady and rhythmic click-click-click of multiple computer keyboards not the rat-a-tat-tat of weapons. The simple fact is that there are far too many people working on the same problems and subjects and duplication and confusion in such hectic environments is almost a given. We are on record as suggesting that this degree of bureaucracy is dysfunctional and counter to the operational need on the ground. There is a joke that routinely circulates around military circles that is not entirely fiction: What is the function of all of these staff officers? To create, of course, the two-hour Microsoft PowerPoint presentations that start every day of operations in Kabul, in IJC and in Regional Commands. Staff are so busy reporting what has happened that what could happen in the future gets drowned out by the noise.

SUMMARY OF OUR CONCLUSIONS

62. In summary, we find we reach rather different conclusions than those of RAND. This is not to say we disagree with RAND's conclusions; we find value in each and every one of them, if not the recommendations. But in our view, RAND's conclusions and the recommendations are too simplistic and evidence of a deficit of deeper thinking over the problem, which is by no means restricted to RAND. For us the key issues are:

- Failure to adapt and evolve.
- Unhealthy over-reliance on attitudinal products.
- The absence of a narrative that Afghans can believe and trust.
- No effort to conduct coherent TAA
- The absence of proper MOE procedures and methodologies.
- Over-reliance upon surveys and polling
- An educational and training deficit at senior levels.
- Complex C2 structures at every level of command and a concomitant dysfunctionality as a direct result

RAND RECOMMENDATIONS

63. Whilst we do not disagree with the conclusions of the RAND report, we believe that they profoundly miss the point and result in faulty recommendations:

- **RAND Recommendation 1**: Hold a conference of IO and PsyOps personnel who have served in Afghanistan to define best practice

Comment: We would not dispute that the sharing of information and good practice is a well-established means of improving outputs and we would not wish to denigrate this. However to place it as the principle recommendation of such a major report suggests a paucity of thinking and encourages group think when actually innovation is necessary.

- **RAND Recommendation 2** : Use local focus groups to pre-test messages

Comment: This is already a principal tenet of UK PsyOps and utilises the services of many locally employed personnel; we would be collectively stunned if this was not also the case for US MISO activities. If it is not, and we are horrified that such a possibility may exist, then we wholeheartedly and unequivocally agree with RAND.

- **RAND Recommendation 3** : Conduct public opinion surveys for TAA and post-testing

Comment: This, in the light of our previous discussions on the utility of polling and surveys is a misnomer and we cannot under any circumstances support this recommendation. It leads us further down an already failed and discredited path. TAA is a discreet scientific discipline practiced by one or two truly expert organisations in the world[21] but routinely laid claim to by every commercial PR and Communication company bidding for government work.

- **RAND Recommendation 4** : Use key communicators to help develop and disseminate messages

Comment: We understand that this recommendation refers to using believable conduits for message dissemination. Again, we are stunned that this may not already be a core tenet of US MISO operations.

- **RAND Recommendation 5**: Harmonise IO doctrine and practice and integrate greater integration between PsyOps and Public Affairs

Comment: Doctrine is only ever a handrail or guide for operations. Whilst doctrine must be consistent, over reliance upon generically written doctrine in specific operational scenarios is not desirable. Operators must be provided with the necessary tools to apply doctrinal principals in different scenarios. It is our view that far too much attention is paid to organisations and processes and far too little to actual operations. Further, we are sceptical at the level at which Public Affairs and PsyOps should be harmonised. Public Affairs exists to inform audiences, and often blanket audiences, about events. Whilst that inform process may influence, Public Affairs engages in no specific TAA activity. Nor does Public Affairs have control over the message or message conduit once released. PsyOps seeks to directly influence discreet target groups through military assets. Any confusion of these two would be highly prejudicial and, as we have already seen, arouse enormous concern.[22]

OUR RECOMMENDATIONS

64. Consider this comment from a private circulation paper produced at the UK's Defence Academy in 2009:

For 300 years, during peacetime, the English/UK Defence Budget has been remarkably consistent at between 2-5% of GDP. At 2-3% GDP – without the running costs of current operations, we cannot sustain the capability to conduct the full spectrum of military operations that we have in the past. To do that we would need 4-5% GDP. Even to maintain our current reduced capabilities and associated minimal structures, Defence needs more money than it is getting. Conclusion: Either we need a serious increase in the Defence Budget or we need to introduce drastic changes in the way we do things. (And most likely, we need a combination of the two)[23].

65. It is our view that properly conducted influence activity, centred on the PsyOps/MISO architecture of western militaries, and using proven scientific techniques, makes this aspiration perfectly possible. Accordingly we have only one recommendation:

US MISO (and wider western military PsyOps) needs to mark the imminent end of the campaign in Afghanistan with a complete halt to current attitudinal practices and conduct a fundamental review of doctrine and operating practices.

66. We started our paper with an analogy from World War One. We make no apologies for using another analogy in the following conclusion: imagine a small child in a remote African village with a stomach disorder. With no medical expertise readily available that child is likely to be treated by the village healer, whom we might call the *Witch Doctor*. That individual may decide that the boy is ill because, for example, the spirit of his dead Grandfather is displeased. The healer may prescribe a 'remedy' to the ailment – perhaps an animal sacrifice, some secret concoction or perhaps some ancient chants. But imagine if a qualified medical doctor happened upon the village. He would apply a scientifically derived diagnostic process and may conclude the boy has a urinary infection or some stomach disorder, easily cured with some tablets or perhaps an injection.

67. Why is this relevant? We believe that ISAF's IO and PsyOps is currently anchored in the 'Witch Doctor' school of medicine. It is now time, in the light of operations in Afghanistan and Iraq, to throw out the metaphorical chicken bones, and in their place inject both innovation and properly grounded science into MISO and IO practices.

STRATEGIC DETERRENCE

68. All too often, when we talk of deterrence, it is in the context of hard military capability, and often nuclear at that. Stopping conflict *before it has started* must be a key tenet of our future national security policy. Alongside international aid, public diplomacy and, yes, military deterrence, we need structures capable of understanding group motivations *before* they materialise into abhorrent or undesired behaviours. This is not PR, advertising or marketing; this is not even conventional Military Intelligence *per se*. This is the science, the proper and hard science, of social psychology and in particular Target Audience Analysis. We need to get a lot smarter at it.

69. During the writing of this paper one of the authors took a taxi driven by an Iranian man in his late 50s. He was an intelligent, well-educated, and mannered Muslim gentleman, whom the author mistook at first as an Afghan. They both talked a bit about the issues facing Afghanistan, and without prompting, the taxi driver turned to his passenger and said: "Do you know where the US went wrong in Afghanistan, why it has been so long, and such a mess? They didn't understand the people, their culture, their ways of behaving. They just went in there and from the start got it all wrong. It's too late to change that now. If they'd spent a billion dollars on research at the beginning, they could have saved themselves trillions, and many lives."

70. We end this paper with two quotations which we think rather nicely sum up the whole problem. The first is attributed to Mark Twain and the second to Alvin Tofler. Both are entirely apt.

"If you do what you have always done you will get what you've always got"

"The illiterate of the twenty-first century will not be those who cannot read and write, but those who cannot learn, unlearn and relearn".

Notes:

1 We very strongly agree with this objective and as scholars such as Galula, MacKinlay and Kilcullen have observed, placing the population at the centre of operational design and activities is central to any successful COIN strategy.

2 http://www.sada-e-azadi.net/

3 'Get the Message Out', The Washington Post, Richard Holbrooke, 28 October 2001.

4 http://people.umass.edu/aizen/f&a1975.html

5 Myers, D. (2010). Social Psychology

6 Available to download at : www.rand.org/pubs/monographs/MG607.html

7 Ries & Trout, Positioning: The Battle for Your Mind. McGraw-Hill, 2000

8 US Info Ops Programmes dubious, costly. USA Today dated 29 Feb 2012.

9 Panel calls for cuts to DoD propaganda spending USA Today 17 May 2012

10 Hartshorne H & May M, *Studies in the Nature of Character* (MacMillan Press), 1928.

11 Paluck, E.L. (2009). *Reducing intergroup prejudice and conflict using the media: A field experiment in Rwanda*. Journal of Personality and Social Psychology, 96, 574-587.

12 This has become a particularly vibrant area of research in recent years and we believe has been under utilized by the armed forces. We note that this is not true across wider [UK] government; No 10 Downing Street now has a behavioural 'nudge' unit attached to it.

13 http://comops.org/journal/page/4/

14 www.icosgroup.net/static/reports/afghanistan_transition_missing_variable.pdf

15 It is also difficult not to note that the 'product' was a DVD. Our experience of Afghan villages in Helmand is that DVD players, and for that matter TVs, are few and far between; so for that matter electricity.

16 Svet, Oleg, "*Fighting for a Narrative: A Campaign Assessment of the US-Led Coalition's Psychological and Information Operations in Afghanistan*," *Small Wars Journal*, September 12, 2010. Available to download at: http://smallwarsjournal.com/blog/2010/09/fighting-for-a-narrative/

17 RAND Corporation, '*US Military Information Operations In Afghanistan: Effectiveness of Psychological Operations 2001-2010*', May 2012, p. 63

18 *In search of how people change: Applications to addictive behaviors*. Prochaska, James O; DiClemente, Carlo C; Norcross, John C. American Psychologist, Vol 47(9), Sep 1992, 1102-1114.

19 Connectivity, War & Beyond Cyber War by David Betz. See: http://kingsofwar.org.uk/2012/11/connectivity-war-beyond-cyber-war/#more-7474

20 http://asiafoundation.org/pdf/Afghan_Report_-April082007.pdf

21 The notoriously conservative US Government Audit Office specifically highlighted the work of the UK's Strategic Communications Laboratories in a report on US public diplomacy and outreach. See *Actions Needed to Improve Strategic Use and Coordination of Research* published by the United States Government Accountability Office. Available to download at: http://www.gao.gov/new.items/d07904.pdf

22 The decision to merge PsyOps and Public Affairs in ISAF's HQ rightly, we believe, caused mass public controversy in 2008 and resulted in the decision being reversed some three days later. *See http://www.reuters.com/article/2008/11/29/us-afghan-nato-idUSTRE4AS0ZV20081129. Press and "Psy Ops" to merge at NATO Afghan HQ*, Reuters, 29 Nov 2008.

23 Realities of Defence Economics. Private circulation paper. UK Defence Academy.

Table of Contents

Hacking the Human Brain: The Next Domain of Warfare

By Chloe Diggins and Clint Arizmendi, Wired, 12.11.12

It's been fashionable in military circles to talk about cyberspace as a "fifth domain" for warfare, along with land, space, air and sea. But there's a sixth and arguably more important warfighting domain emerging: the human brain.

This new battlespace is not just about influencing hearts and minds with people seeking information. It's about involuntarily penetrating, shaping, and coercing the mind in the ultimate realization of Clausewitz's definition of war: compelling an adversary to submit to one's will. And the most powerful tool in this war is brain-computer interface (BCI) technologies, which connect the human brain to devices.

Current BCI work ranges from researchers compiling and interfacing neural data such as in the Human Conectome Project to work by scientists hardening the human brain against rubber hose cryptanalysis to technologists connecting the brain to robotic systems. While these groups are streamlining the BCI for either security or humanitarian purposes, the reality is that misapplication of such research and technology has significant implications for the future of warfare.

Where BCIs can provide opportunities for injured or disabled soldiers to remain on active duty post-injury, enable paralyzed individuals to use their brain to type, or allow amputees to feel using bionic limbs, they can also be exploited if hacked. BCIs can be used to manipulate … or kill.

Recently, security expert Barnaby Jack demonstrated the vulnerability of biotechnological systems by highlighting how easily pacemakers and implantable cardioverter-defibrillators (ICDs) could be hacked, raising fears about the susceptibility of even life-saving biotechnological implants. This vulnerability could easily be extended to biotechnologies that connect directly to the brain, such as vagus nerve stimulation or deep-brain stimulation.

Outside the body, recent experiments have proven that the brain can control and maneuver quadcopter drones and metal exoskeletons. How long before we harness the power of mind-controlled weaponized drones – or use BCIs to enhance the power, efficiency, and sheer lethality of our soldiers?

Given that military research arms such as the United States' DARPA are investing in understanding complex neural processes and enhanced threat detection through BCI scan for P300 responses, it seems the marriage between neuroscience and military systems will fundamentally alter the future of conflict.

And it is here that military researchers need to harden the systems that enable military application of BCIs. We need to prevent BCIs from being disrupted or manipulated, and safeguard against the ability of the enemy to hack an individual's brain.

The possibilities for damage, destruction, and chaos are very real. This could include manipulating a soldier's BCI during conflict so that s/he were forced to pull the gun trigger on friendlies, install malicious code in his own secure computer system, call in inaccurate coordinates for an air strike, or divulge state secrets to the enemy seemingly voluntarily. Whether an insider has fallen victim to BCI hacking and exploits a system from within, or an external threat is compelled to initiate a physical attack on hard and soft targets, the results would present major complications: in attribution, effectiveness of kinetic operations, and stability of geopolitical relations.

Like every other domain of warfare, the mind as the sixth domain is neither isolated nor removed from other domains; coordinated attacks across all domains will continue to be the norm. It's just that military and defense thinkers now need to account for the subtleties of the human mind … and our increasing reliance upon the brain-computer interface.

Regardless of how it will look, though, the threat is real and not as far away as we would like – especially now that researchers just discovered a zero-day vulnerability in the brain.

Table of Contents

Cyber Security Hunter Teams Are the Next Advancement in Network Defense

Posted by Matthew Rosenquist in Open Port IT Community on Nov 28, 2012

Hunter teams are emerging as a new tool in the world of cyber defense. Computer security continues to improve and evolve of overtime. One of the latest practices gaining momentum is the use of cyber security "Hunter teams". Differing from how standard security operations function, hunter teams fill an important gap and push us one step further on the evolutionary ladder of cyber security. They are cyber-investigators which enhance an organization's capabilities by supplementing the overall defense from persistent attackers. They are typically a group of bright, experienced, talented, and motivated professionals which work together to detect, identify, and understand an advanced and determined threat agent.

Hunter teams approach threats in a personal way. They seek the human origins of attacks and focus their attention on disruption or removal of those threat agents, instead of the attacks themselves. In simple terms, they target the attackers.

These hunter teams are sprouting and taking root in many different places. Anti-malware companies, research organizations, and internal security departments have begun to embrace looking for the attackers. Investigation teams, including cyber guns-for-hire which are brought in after the fact when serious breaches are detected, are also looking for the people behind the attacks. However, it has been the military and sensitive government organizations which have been most vocal in recruiting for hunter team talent. They have the long history of knowing the value of identifying the enemy and have been quick to embrace this practice and are serious in making it successful.

Hundreds of years ago Sun Tsu penned the authoritative tome on warfare strategy. One of its pillars is to know your enemy. A key to conflict is to understand that attacks are simply a method for the threat agent to achieve their objectives. An active defense not only shields against attacks, but also targets the attackers. Those people who would do you or your mission harm. Take the attackers out of the equation and the attacks also go away.

Hunter teams play an important role, different than standard security operations staff. In the past decade, we have seen the rise of security operations centers (SOC). Security operations departments are typically configured, resourced, and driven to contain attacks and remediate to a state of normal operations. They are in a continuous cycle of fixing the symptoms and tweaking the defenses so the organization continues to operate in a stable and expected manner. It is a never ending struggle which works best against the flood of broadly sweeping attacks on the internet, which look for any target of opportunity. In most cases, SOC's are only interested in attacks which undermine the operational performance and value of the environment under their protection. They are well suited to tackle ordinary malware infections or plug understood exploit activities by using industry best-known-practices, but can easily falter when faced with something unique and specifically targeting only them. They are by design inwardly focused, limited to a technology sandbox of security control configuration or fixing assets within their internal environment.

Hunter teams take a different approach and seek the root cause, namely the threat agent themselves, who are initiating one or more attacks. This may be internal or external to the organization. Not satisfied with simply undermining the latest infraction, they want to quell the problem at the source and eliminate future attacks from the same threat agent, whom may possess the ability to coordinate completely unique and unpredictable maneuvers.

History shows why this is important. Attackers maintain the combat initiative and determine where, when, and by what method an attack will occur. Defenders typically respond to attacker's moves and evolve the defenses to protect against those newly understood methods.

Attackers therefore have an advantage. It takes time, effort, and resources for defenders to recognize they are being attacked, decipher how it is being done, then develop a means to isolate the ongoing breach and block future attacks, and then remediate the affected systems. A threat agent who is determined to attack a specific target can try a number of methods until they succeed. Without threat of themselves being in jeopardy, they can continue varying the assault until they find an approach which works. The only effective way to stop such a persistent threat agent is to dissuade or remove them from the equation. This is where the hunter teams come into play.

Criminal investigators are a good example of the hunter team methodology at work. If someone breaks down a door to rob a bank, the security operations team looks to install stronger doors and maybe a better alarm system. They are inclined to identify and close the vulnerability. A criminal investigator will look to see who is trying to rob banks and target those threat agents. The investigator knows such a robber will continue to evolve their tactics until they succeed. Operations efforts to improve door standards, alarms, etc. are still fine measures which reduce the risk of loss, but the investigator's role is just as important.

When I managed Intel's Security Operations Center, I was also the Incident Commander for the company's IT Emergency Response Process. This is the team that takes charge whenever the company's computer environment is being attacked. I remember during a virus outbreak instructing the security operations team to track, isolate, and clean infected systems, and then turning to my intelligence section leader and asking him to go forth and determine whether the incident was simply a wild virus finding its way through the cracks or was it a directed attack specifically against our company. The challenge I assigned the intelligence lead was so I could understand if the threat agent was specifically targeting Intel Corp with their malicious attacks or if we were simply caught in a broader net cast with a generic attack. This would help me understand whether it was a fluke oversight in the configuration of our defenses or just the beginning of something far worse, potentially a directed campaign against our security infrastructure.

Cost and scalability limits will constrain their use, but hunter teams are an important step forward for the industry. Cyber security hunter teams have been in limited use for some time and are gaining momentum. The results can be seen in the news. Botnet takedowns, the breaking-up carding rings, shutting down of illegal fraud sites, malware author arrests, and the prosecution of insider theft and sabotage cases are possible because the attackers were targeted. What are not publicized are the equally impressive results which occur quietly in defense of highly protected networks. These teams can be valuable in identifying the root cause of problems, putting the puzzle pieces of seemingly disparate incidents together, identifying the offending attackers, reconnaissance for early alerting, and providing intelligence necessary to interdict and prosecute them. Hunter teams can be a very powerful tool and effective in stopping some of the most grievous threats.

These specialized capabilities come at a cost. In order to succeed, a combination of brilliant talent, tools, support from legal, and in some cases partnership with law enforcement and industry partners/suppliers/customers, is required. It is a significant investment to establish and maintain a team at a sufficient level to see worthwhile results. Additionally, something intangible is needed; patience. Even the most proficient team needs time to hunt and results can vary greatly.

Beyond costs, hunter teams also have a significant downside. They are not very scalable. Most teams work a single case or issue to closure. Some teams can multi-task, but at a great loss of effectiveness. I have been fortunate to be a part of a world class loss prevention team, specializing in detecting, tracking and prosecuting threat agents. When on the hunt, teams are narrowly focused. Timing is critical. Proficiency matters. Splitting attention to a multitude of separate cases is a recipe for disaster. Compared to security operations teams, which can much more easily multitask and close issues with great speed, hunter teams seem to move in slow motion. But what they lack in the quantity of case closures, they can make up for in results. Overall, the high costs and the lack of scalability are tall barriers which prevent widespread adoption.

Certain organizations, where the cost and scalability headaches are worth the additional security capabilities, should consider the use of hunter team's. Environments where assets are targeted by persistent, creative, and resourceful threat agents, seeking explicit objectives, from a specific target will benefit the most. Identifying and understanding these dangerous and capable adversaries, who seek to undermine your security controls and compromise your environment, is an important step in countering massive potential damage. This is not important to most, but for those organizations which are under the pressure of being targeted directly by skillful and motivated threat agents, hunter teams are a viable and attractive option. I strongly suggest financial, defense, sensitive government, and high profile critical infrastructure organizations look into using them. Additionally, I urge security providers and consulting firms to evaluate offering professional hunter team services. The demand over time will continue to grow.

Hunter teams are a necessity in the evolution of cyber security. They are a pivotal step forward, applying desired pressure to attackers. Yet, they are not the final state. We will continue to evolve the practices and technology of targeting threat agents into something more scalable, affordable, and effective. But for the time being, I welcome hunter teams to the playing field. It is about time you showed up. We really need you. Happy hunting!

Table of Contents

Hype and Fear

From the Economist, Dec 8th 2012

EVEN as anxiety about jihadi terrorist threats has eased, thanks to the efforts of intelligence agencies and drone attacks' disruption of the militants' sanctuaries, fears over Western societies' vulnerability to cyber-assaults have grown. Political and military leaders miss no chance to declare that cyberwar is already upon us. America's defence secretary, Leon Panetta, talks of a "cyber-Pearl Harbour". A senior official says privately that a cyber-attack on America that "would make 9/11 look like a tea party" is only a matter of time.

The nightmares are of mouseclicks exploding fuel refineries, frying power grids or blinding air-traffic controllers. The reality is already of countless anonymous attacks on governments and businesses. These seek to disrupt out of malice, or to steal swathes of valuable commercial or security-related data. Some experts believe that such thefts have cost hundreds of billions of dollars in stolen R&D.

Many of these attacks are purely criminal. But the most sophisticated are more often the work of states, carried out either directly or by proxies. Attribution—detecting an enemy's fingerprints on a cyber-attack—is still tricky, so officials are reluctant to point the finger of blame publicly. But China is by far the most active transgressor. It employs thousands of gifted software engineers who systematically target technically advanced Fortune 100 companies. The other biggest offenders are Russia and, recently, Iran (the suspected source of the Shamoon virus that crippled thousands of computers at Saudi Arabia's Aramco and Qatar's RasGas in August).

America and its allies are by no means passive victims. Either America, Israel or the two working together almost certainly hatched the Stuxnet worm, found in 2010, that was designed to paralyse centrifuges at Iran's Natanz uranium-enrichment plant. The Flame virus, identified by Russian and Hungarian experts this year, apparently came from the same source. It was designed to strike at Iran by infecting computers in its oil ministry and at targets in the West Bank, Syria and Sudan.

Boring, not lurid

For all the hype, policies on cyber-warfare remain confused and secretive. The American government is bringing in new rules and a clearer strategy for dealing with cyber-threats. Barack Obama is said to have signed in October a still-secret directive containing new guidelines for federal agencies carrying out cyber-operations. It sets out how they should help private firms, particularly those responsible for critical national infrastructure, to defend themselves against cyber-threats by sharing information and setting standards.

The directive is partly a response to the stalling of cyber-legislation in the Senate. Republican senators argue that it imposes too great a regulatory burden on industry, which is already obliged to disclose when it is

subject to a cyber-attack. It is also meant to govern how far such bodies as the Department of Homeland Security can go in their defence of domestic networks against malware attacks.

The Pentagon is also working on more permissive rules of engagement for offensive cyber-warfare, for example to close down a foreign server from which an attack was thought to be emanating. General Keith Alexander heads both Cyber Command (which has a budget of $3.4 billion for next year) and the National Security Agency. He has often called for greater flexibility in taking the attack to the "enemy". The emergence of new cyber-warfare doctrines in America is being watched closely by allies who may follow where America leads—as well as by potential adversaries.

However, Jarno Limnell of Stonesoft, a big computer security firm, says that all levels of government in the West lack strategic understanding on cyber-warfare. So, although questions abound, answers are few. For example, it is not clear how much sensitive information about threats or vulnerabilities government agencies should share even with private-sector firms that are crucial to national security. Often the weakest link is their professional advisers, such as law firms or bankers who have access to sensitive data.

Almost all (roughly 98%) of the vulnerabilities in commonly used computer programmes that hackers exploit are in software created in America. Making private-sector companies more secure might involve a controversial degree of intrusion by government agencies, for example the permanent monitoring of e-mail traffic to make sure that every employee is sticking to security rules. Government hackers may also like to hoard such vulnerabilities rather than expose them. That way they can later create "backdoors" in the software for offensive purposes.

Also controversial is the balance between defence and attack. General Alexander stresses that in cyber-warfare, the attacker has the advantage. Mr Limnell says that, although America has better offensive cyber-capabilities than almost anybody, its defences get only three out of ten.

Setting rules for offensive cyber-warfare is exceptionally tricky. When it comes to real, physical war, the capability may become as important as air superiority has been for the past 70 years: though it cannot alone bring victory, you probably can't win if the other side has it.

China has long regarded the network-centric warfare that was developed by America in the late-1980s and copied by its allies as a weakness it might target, particularly as military networks share many of the same underpinnings as their civilian equivalents. The People's Liberation Army (PLA) talks about "informationisation" in war, "weakening the information superiority of the enemy and operational effectiveness of the enemy's computer equipment". China's planning assumes an opening salvo of attacks on the enemy's information centres by cyber, electronic and kinetic means to create blind spots that its armed forces would then be able to exploit. Yet as the PLA comes to rely more on its own information networks it will no longer enjoy an asymmetric advantage. Few doubt the importance of being able to defend your own military networks from cyber-attacks (and to operate effectively when under attack), while threatening those of your adversaries.

But to conclude that future wars will be conducted largely in cyberspace is an exaggeration. Martin Libicki of the RAND Corporation, a think-tank, argues that with some exceptions cyber-warfare neither directly harms people nor destroys equipment. At best it "can confuse and frustrate…and then only temporarily". In short, "cyber-warfare can only be a support function" for other forms of war.

Four horsemen

Besides the cyber element of physical warfare, four other worries are: strategic cyberwar (direct attacks on an enemy's civilian infrastructure); cyber-espionage; cyber-disruption, such as the distributed denial-of-service attacks that briefly overwhelmed Estonian state, banking and media websites in 2007; and cyber-terrorism. Gauging an appropriate response to each of these is hard. Mr Limnell calls for a "triad" of capabilities: resilience under severe attack; reasonable assurance of attribution so that attackers cannot assume anonymity; and the means to hit back hard enough to deter an unprovoked attack.

Few would argue against improving resilience, particularly of critical national infrastructure such as power grids, sewerage and transport systems. But such targets are not as vulnerable as is now often suggested. Cyber-attacks on physical assets are most likely to use what Mr Libicki calls "one-shot weapons" aimed at industrial control systems. Stuxnet was an example: it destroyed perhaps a tenth of the Iranian centrifuges at Natanz and delayed some uranium enrichment for a few months, but the vulnerabilities it exposed were soon repaired. Its limited and fleeting success will also have led Iran to take measures to hinder future attacks. If that is the best that two first-rate cyber-powers can do against a third-rate industrial power, notes Mr Libicki, it puts into perspective the more alarmist predictions of impending cyber-attacks on infrastructure in the West.

Moreover, anyone contemplating a cyber-attack on physical infrastructure has little idea how much actual damage it will cause, and if people will die. They cannot know if they are crossing an adversary's red line and

in doing so would trigger a violent “kinetic” response (involving real weapons). Whether or not America has effective cyber-weapons, it has more than enough conventional ones to make any potential aggressor think twice.

For that reason, improving attribution of cyber-attacks is a high priority. Nigel Inkster, a former British intelligence officer now at the International Institute for Strategic Studies, highlights the huge risk to the perpetrator of carrying out an infrastructure attack given the consequences if it is detected. In October Mr Panetta said that “potential aggressors should be aware that the United States has the capacity to locate them and hold them accountable for actions that harm America or its interests.”

He may be over-claiming. Given that cyber-attacks can be launched from almost anywhere, attribution is likely to remain tricky and to rely on context, motive and an assessment of capabilities as much as technology. That is one reason why countries on the receiving end of cyber attacks want to respond in kind—ambiguity cuts both ways. But poor or authoritarian countries attacking rich democratic ones may not have the sorts of assets that are vulnerable to a retaliatory cyber-attack.

The difficulty is even greater when it comes to the theft (or “exfiltration”, as it is known) of data. For China and Russia, ransacking Western firms for high-tech research and other intellectual property is tempting. The other way round offers thinner pickings. In 2009 hackers from an unnamed “foreign intelligence agency” made off with some 24,000 confidential files from Lockheed Martin, a big American defence contractor. As a result they could eavesdrop on online meetings and technical discussions, and gather information about the sensors, computer systems and “stealth” technology of the F-35 Joint Strike Fighter. This may have added to the delays of an already troubled programme as engineers tried to fix vulnerabilities that had been exposed in the plane’s design. Investigators traced the penetrations with a “high level of certainty” to known Chinese IP addresses and digital fingerprints that had been used for attacks in the past. Less than two years later, China unveiled its first stealth fighter, the J-20.

Theft from thieves

As Mr Libicki asks, “what can we do back to a China that is stealing our data?” Espionage is carried out by both sides and is traditionally not regarded as an act of war. But the massive theft of data and the speed with which it can be exploited is something new. Responding with violence would be disproportionate, which leaves diplomacy and sanctions. But America and China have many other big items on their agenda, while trade is a very blunt instrument. It may be possible to identify products that China exports which compete only because of stolen data, but it would be hard and could risk a trade war that would damage both sides.

Cyber-disruption has nuisance value and may be costly to repair, but it can be mitigated by decent defences. Cyber-terrorism has remained largely in the imagination of film-makers, but would be worth worrying about if it became a reality. Stonesoft’s Mr Limnell reckons that, though al-Qaeda and its offshoots show little sign of acquiring the necessary skills, they could buy them. Mr Libicki is more sceptical. Big teams of highly qualified people are needed to produce Stuxnet-type effects, which may be beyond even sophisticated terrorist groups. Also, the larger the team that is needed, the more likely it is to be penetrated.

The Obama administration’s attempt to develop a more coherent—and perhaps less secret—doctrine of cyber-warfare is sensible so long as it is not just an excuse for hyping something that, as far as is known, has yet to kill anybody. The idea that offence beats defence is also suspect. If more attention were paid to fixing the security flaws in Western software, cyber-attackers would have fewer entry points. And more effort should be put into solving the attribution problem. Getting caught is a deterrent that state actors take seriously. But given that the essence of cyber-warfare is ambiguity and uncertainty, gaining clarity and certainty will be exceptionally difficult. That makes policy both hard to construct and harder still to explain.

Table of Contents

ARCYBER on the Attack on Paper, In Training

By Joe Gould, DefenseNews, 18 Dec 2012

One day an Army brigade may call for a cyber attack as it does for a precision-guided bomb, according to an official with Army Cyber Command.

The military is figuring out the chain of authorities a commander might use to trigger an offensive attack — a kind of cyber effects request system, according to Col. Thomas Goss, chief of the command’s Strategic Initiatives Group.

Eventually, Goss said, the ability to coordinate cyber operations through a brigade’s intelligence, communications and operations personnel, and higher echelons, will be organic to a brigade.

ARCYBER is working on a basic set of instructions for a brigade or division commander that would outline "certain effects that he would want," Goss said.

Brigades themselves would not receive any sort of hacker tools. Instead, Goss said, the process would be similar to the chain of authorities used to approve a joint fires strike.

"As you can imagine, with an emerging domain and an emerging operational dynamic, those authorities are not delegated down to the lowest levels," Goss said. "If you picture the equivalent of joint fires, somehow we have figured out how a division or brigade commander drops a [Joint Direct Attack Munition] where they want it without giving them an airplane."

Goss declined to give details about specific effects in an unclassified forum.

As the Army works on writing the doctrine, ARCYBER has placed an emphasis on personnel, training and leadership development.

Emerging fast

Cyber training is getting a jump-start as the Army includes network warfare scenarios in a growing number of brigade-level and division-level exercises.

To teach soldiers better cybersecurity practices, the Army has fielded an opposition force that models enemy capabilities in combat training at the National Training Center at Fort Irwin, Calif., and at the Joint Readiness Training Center at Fort Polk, La.

The "World Class Cyber OPFOR," fielded by 1st Information Operations Command, can act out a range of scenarios, from fishing for information on poorly guarded networks to attacking the brigade's mission command systems.

"What we are looking for is basically to approximate what threat or adversary the OPFOR commander is modeling, so we have tiers of adversary capabilities," Goss said.

The idea is to expose vulnerabilities and improve the cybersecurity practices of the training unit.

After an exercise, the cyber red team's commander can describe for the blue force what his objectives were and what he achieved. The brigade is shown what sensitive information it may have left unsecured, how it was discovered and how it was used against the unit.

"That allows my commander not just to have a talk with the OPFOR commander but ask, 'How did you learn this? How did you get these graphics? Why did this system ... get to slower and slower when the battle went on?'" Goss said. "It also allows him to interact with his staff to say, 'How can we prevent this from happening again?'"

Goss said after the cyber red team's inclusion in three cycles at NTC and one at JRTC, commanders have been quick to catch on. Without a good cybersecurity training program and an awareness of their networks, commanders will lose their freedom to operate on the battlefield and fail.

These scenarios are fueling questions at the Tactical Commander's Development Program at Fort Leavenworth, Kan., which in turn are "energizing" discussions over the evolving "doctrinal toolkit" for cyber, Goss said.

An ongoing capabilities-based assessment for cyber operations, led by Training and Doctrine Command, is incorporating lessons learned from such brigade-level exercises and 20 major exercises in which ARCYBER participates.

Table of Contents

Electronic Warfare Graduates First To Receive Crested Collar Insignia

By Cannoneer staff, US Army homepage,December 19, 2012

FORT SILL, Okla. (19 Dec. 2012) -- Twenty-eight Soldiers in the Electronic Warfare Specialist Basic Course were the first students to receive the new Electronic Warfare, or EW, collar insignia at a graduation and cresting ceremony, Dec. 13, at Fort Sill.

Students in Class No. 001-13 were pinned by warrant officers currently in the EW Technician Warrant Officer Basic Course. Keynote speaker Col. John Smith, Fires Center of Excellence Joint and Combined Integration Directorate director, spoke to the graduates about the impact of Military Occupational Specialty, or MOS, 29E, and the meaning of the collar device.

"The role electronic warfare has played in Iraq and Afghanistan has been very significant," said Smith. "Many of our adversaries are now challenging U.S. forces' dominance of the electromagnetic spectrum on a daily basis. That's where your newly honed skills, abilities and knowledge will come into play."

A crest identifies a Soldier's MOS, and inside the crest are symbols that describe a Soldier's duties. The EW crest features a lightning bolt, key and shield.

The lightning bolt represents the Army's intent to rapidly, decisively and precisely strike at the adversary with an electronic attack. The key symbolizes the means by which Soldiers unlock access to knowledge of the adversary, and the safekeeping of friendly capabilities and knowledge through electronic support and protection. The shield represents the unconditional commitment to electronically protect people, information and equipment from danger and harm.

Together they represent the Army's commitment to control the electromagnetic spectrum to gain and maintain the advantage in the operational environment, Smith said.

As the sole EW subject-matter expert at many units, these Soldiers will be relied on by battalion commanders to guide them on how best to employ electronic warfare, Smith said. The EW Soldiers should respond to this call of duty aggressively, tirelessly and be well-prepared, he said.

EW specialists plan and integrate EW support into a ground combatant commander's operations, said Lt. Col. Steven Oatman, Army Electronic Warfare School director.

One example would be electronic jamming of an adversary's radio-controlled improvised electronic devices without disrupting U.S. forces' communications in a maneuver (ground) operation, Oatman said. EW specialists are assigned at the battalion level and up to combatant commands across the Army.

Many of the students in the nine-week course were changing MOSs (reclassifying) from over-strength jobs to EW, which is understrength, said Sgt. 1st Class Michael Fleury, 29E lead instructor. The EW mission falls under the field artillery branch.

Seventeen of the graduates were National Guard Soldiers because the Guard and Reserve are supplementing the active component, as well as meeting the requirement to have a certain number of 29Es in their battalions or brigades, said Fleury, a former communications specialist. All of the graduates will go to deploying units.

Graduate Sgt. Stephen Applebee, Vermont Army National Guard, said he reclassified to EW because there was a position open at his brigade.

"It's a much-needed career field for the Army because of the technology and information in warfare," said Applebee, who is an Active Guard Reserve Soldier.

Table of Contents

How to Equip the U.S. Military for Future Electronic Warfare

By Rich Sorelle, National Defense Magazine, January 2013

As the U.S. military pivots away from counterinsurgency campaigns, it will confront different challenges and strategic environments.

In Iraq, forces commanded the skies, and forward operating bases and computer systems remained secure. Coalition troops enjoyed freedom of movement. In Afghanistan, the U.S. military outmatches the Taliban.

But we may lack these advantages in a future conflict.

The next time around, the nation may see adversaries mining critical waterways or attacking offshore staging areas with long-range missiles, all in an anti-access effort designed to make U.S. power projection very costly. Likewise, area denial tactics, such as radio frequency (RF) jamming, may hamstring U.S. forces already in theater. Taken together, anti-access/area denial (A2/AD) is a serious challenge that must be addressed.

In response, the Navy and Air Force have adopted “air-sea battle.” The concept entails highly coordinated, cross-domain operations designed to “disrupt the adversary’s intelligence collection and command and control used to employ A2/AD weapons systems; destroy or neutralize A2/AD weapons systems within effective range of U.S. forces; and defeat an adversary’s employed weapons to preserve essential U.S. joint forces and their enablers,” according to the air-sea battle office.

Much of this involves employing the right mix of kinetic weapons. But planners also need to appreciate the critical role of electronic warfare, both in how U.S. adversaries have rolled it into their A2/AD strategies and how our military must use it to maintain freedom of movement and force projection.

Now, it's tempting, given the current budgetary environment, for defense planners to look to electronic warfare systems to make cuts. But that would be shortsighted. The electronic warfare community, both industry and government, needs to rally and make clear what is at stake. There will be no air-sea battle without the tools necessary to control the electromagnetic spectrum across land, sea, air, space and cyberdomains.

As it stands now, the United States no longer enjoys spectrum dominance. In a February statement submitted to the House subcommittee on emerging threats and capabilities, then-deputy director of the Defense Advanced Research Projects Agency Kaigham Gabriel noted that over the past 15 years, other nations have exploited advances in consumer electronics to catch up in electronic warfare.

Microelectronic devices are not just shrinking, Gabriel explained. They are now able to match U.S. military performance levels. Likewise, signal-processing chips are being replaced by programmable chips, which can be produced more easily and be configured to offer much the same capability as military grade hardware. Finally, Gabriel noted, the explosion of mobile communications has had a lasting effect on electronic warfare, providing state-of-the-art, miniaturized processing technology to anyone who can reverse engineer a cell phone.

Every day, we see this leveling effect in spectrum capabilities. For example, North Korea has employed truck-mounted, long-range jammers to repeatedly drown out GPS satellite signals in many parts of South Korea. One such attack in late April and early May affected the navigation systems of 337 commercial airliners, 122 ships and even cars driving around the streets of Seoul.

This vulnerability extends to defense systems as well. Last March, Pyongyang's disruption of GPS signals forced a U.S. Army reconnaissance aircraft to make an emergency landing. Then, several months later, the Iranians captured the advanced RQ-170 drone by, they claim, first cutting its communications link and then spoofing the autopilot's return coordinates.

When the story of the RQ-170 first broke, many doubted Iran could pull off such a technological feat. But University of Texas at Austin researchers have since proven that drones using unencrypted signals can indeed be hacked. To take control of the RQ-170, an enemy would have to cause the drone's communications to switch from the encrypted P(Y) code to the civilian C/A code, theorized Richard Langley, a GPS expert at the University of New Brunswick.

It doesn't take a lot of imagination to see what role electronic warfare would play in a larger A2/AD posture. The enemy could degrade the accuracy of U.S. precision-guided munitions or attack other systems. Finally, do not forget that surface-to-air missile batteries would be useless without radars to zero in on aircraft.

The U.S. military and defense industry have started addressing some of these spectrum issues. For example, the Marine Corps has been placing the jam-resistant Link 16 on some of its drones. Likewise, the new GPS III satellites — set to begin launching in 2014 — will broadcast M-code, a far stronger, more secure military signal than P(Y). Advances are also being made in free space optical communications devices, also known as laser communications, which are harder to intercept than RF-based communications. (See story page 34.)

The Defense Department needs to determine what effective electronic warfare systems the military could bring to bear in air-sea battle. Here, there are actually quite a few options. For instance, various airborne jamming systems can blind enemy air defense radar and interfere with his communications, data and computer networks, giving U.S. forces maximum room to maneuver in territory otherwise denied to them.

One such technology is the U.S. Navy's next-generation jammer (NGJ), which is being developed for use on the carrier-based EA-18G Growler and other aircraft, such as unmanned aerial vehicles. It will embrace the latest in RF technology and have an open architecture. This means that pilots will deliver more jamming power against more targets with more precision — and continue to do so long into the future.

Just as NGJ will clear a safe path for U.S. and allied aircraft, minesweepers can disrupt A2/AD by neutralizing threats in disputed waterways. Cheap and effective, mines let even a small power hold the world's navigation hostage. But systems like helicopter-towed sweeps, which use acoustic and magnetic fields to set off influence mines at a safe distance, are proving once again the utility of electronic warfare.

These are just some of the technologies that will help the nation maintain its edge in the next conflict. But that assumes that proper investments will be made. The key message for decision makers is that electronic warfare is going to be a prominent feature of both A2/AD and air-sea battle. Ignoring the electromagnetic spectrum is not an option.

Table of Contents

Al-Qaida Hit by Cyber Attack

By J.J. Green, wtop.com, 12/19/2012

WASHINGTON - Key al-Qaida websites were knocked offline more than two weeks ago and are still dark, according to U.S. intelligence sources.

This is one of the longest disruptions the organization has experienced since it set up its online distribution system in 2006. Al-Qaida also was hit by a massive cyber attack in late 2008, from which the online network never recovered.

Intelligence sources say the most recent attack has significantly inhibited the organization's ability to recruit online and post propaganda and is the second blow to the organization's recruiting just this month.

The return of al-Qaida in Iraq was supposed to be hailed by a flood of propaganda from the al-Qaida online network, but the sites went dark in early December after the cyber attack.

A film called "Salil al-Sawarim 3" was scheduled to be released last week to announce the return. Online jihadists had been discussing the release for more than a month, and had been sharing images and footage from the production.

But the blackout has delayed the release and, according to U.S. intelligence sources, left sympathizers scrambling to find a way to communicate.

Al-Qaida has been using the websites to post propaganda that experts say is successfully radicalizing youth all over the world, including in Syria where the organization is believed to be active.

Intelligence sources say the blackout has spurred an influx of al-Qaida-related messages on Twitter. Because key jihadist sites have been disrupted, there are no trusted locations where sympathizers can congregate and communicate.

"The al-Qaida organization was trying to inspire organizations in other groups around the world to conduct attacks as al-Qaida would've wanted them to conduct attacks," says Philip Mudd, a senior global analyst at Oxford Analytica.

Blow to Syria operations

The cyber attack comes as the U.S. State Department, according to a senior official, has "formally amended al-Qaida in Iraq as a Foreign Terrorist Organization."

Through a department executive order, the designation now includes the alias al-Nusrah Front, which is part of al-Qaida in Iraq. Al-Qaida in Iraq was first designated as a foreign terrorist organization by the State Department in October 2004.

Designating al-Nusrah as a terrorist organization places sanctions on the organization, making any funds or assistance directed to the organization illegal. The designation is generally recognized by U.S. allies and all who oppose al-Qaida, making it harder for the organization to raise money.

The amended designation could hinder terror cell operations in Syria as well.

"Since November 2011, al-Nusrah Front has claimed hundreds of attacks, nearly 600, in major city centers across Syria in which numerous innocent Syrians have been injured and killed. (Al-Qaida) has dispatched money, people, and material from Iraq to Syria over the past year to attack Syrian forces both on its own initiative

Table of Contents

Chinese Hackers Suspected in Cyber Attack on Council on Foreign Relations

By Bill Gertz, Washington Free Beacon, December 27, 2012

Computer hackers traced to China carried out an advanced cyberespionage attack against one of America's most elite foreign policy web groups – the website of the Council on Foreign Relations (CFR).

According to private computer-security forensic specialists, the hacking incident involved a relatively new type of ploy called a "drive-by" website cyber attack that was detected around 2:00 p.m. on Wednesday.

The specialists, who spoke on condition of anonymity, said the attack involved penetrating the computer server that operates the New York City-based CFR's website and then using the pirated computer system to attack CFR members and others who visited or "drove by" the site.

The activity ended on Thursday and the specialists believe the attackers either removed their malicious software to prevent further details of the attack from being discovered, or CFR was able to isolate the software and remove it.

The FBI was notified of the attack and is said to be investigating.

FBI spokeswoman Jennifer Shearer declined to comment when asked about the attack. But she told the Washington Free Beacon: “The FBI routinely receives information about threats and takes appropriate steps to investigate those threats.”

However, David Mikhail, a Council on Foreign Relations spokesman, confirmed the attack. “The Council on Foreign Relations’ website security team is aware of the issue and is currently investigating the situation,” Mikhail said in an email. “We are also working to mitigate the possibility for future events of this sort.” He provided no details.

According to the computer security specialists, the cyber espionage attack represents a new level of sophistication by foreign hackers seeking government and other secrets by computer.

The method used in a “drive-by” attack requires hackers to covertly plant malicious software in the CFR computer system. Then, they used the software and the web site to attack visitors to the site by infecting their computers in a hunt for secrets and other valuable information. One of the specialists said the attack also involved using the CFR site for what is called a “watering hole” attack, when people who visit the website are infected.

One of the victims who visited the CFR’s website, cfr.org, discovered the attack and alerted computer security specialists on Wednesday.

In response, a small group of private security specialists launched an investigation into the activity and found that it only targeted computer users using the web browser Windows Internet Explorer 8 and higher versions. The attackers were able to exploit a security flaw in the browser software called a “zero-day” vulnerability – a previously unknown flaw that allows computer hackers to gain access to a targeted computer.

A similar Internet Explorer vulnerability was behind the major Aurora cyber attack on Google and other U.S. corporations that began in 2009 and was traced to China’s government.

Investigators said the computer attackers that targeted CFR were able to set up a covert network capable of identifying, encrypting, and sending stolen information found in targeted and infected computers back to a secret command and control computer.

In the case of the CFR hack, the malicious software involved software that included Mandarin Chinese language, the specialists said. Also, the attackers limited their targeting to CFR members and website visitors who used browsers configured for Chinese language characters – an indication the attackers were looking for people and intelligence related to China.

“This was a very sophisticated attack,” said one of the specialists. “They were looking for very specific information from specific people.”

The extent of the damage is not known but CFR members who visited the website between Wednesday and Thursday could have been infected and their data compromised, the specialists said.

The CFR is one of the most elite foreign policy organizations in the United States with a membership of some 4,700 officials, former officials, journalists, and others. Its members include NBC anchor Brian Williams, Hollywood actress Angelina Jolie, and former Sen. Chuck Hagel, President Obama’s embattled but as yet un-nominated choice for secretary of defense.

Current Secretary of State Hillary Clinton and Assistant Secretary of State Kurt Campbell, the Obama administration’s senior Asian affairs policy maker, also are CFR members. Senate Intelligence Committee Chairman Sen. Dianne Feinstein (D., Calif.) is also a member, as is Secretary of State-designate Sen. John Kerry.

Its board and members include a who’s who of U.S. foreign policy and national security elites, including former U.S. Central Command commander Army Gen. John Abizaid, and former Secretaries of State Madeleine K. Albright, Colin Powell, and Henry Kissinger.

Fox News CEO Roger Ailes also is a member, as is News Corp. chairman and CEO Rupert Murdoch. Former Presidents George W. Bush and Bill Clinton are members, as is former CIA Director and former Defense Secretary Robert M. Gates and former CIA Director David Petraeus.

The CFR cyberstrike is not the first strategic drive-by cyber attack.

The computer security website Dark Reading reported in May that the Center for Defense Information, and the Hong Kong chapter of the human rights group Amnesty International (AIHK), along with several other organizations, also were attacked using similar drive-by methods.

"The weapon of choice for a cyberspy or advanced persistent threat (APT) actor gaining a foothold inside its target traditionally has been the socially engineered email with a malicious link or attachment," DarkReading stated. "But cyberspies are increasingly targeting specific, legitimate websites and injecting them with malware in hopes of snaring visiting victims from organizations from similar industries and sectors."

Table of Contents

You Can't Handle the Truth

From Strategy Page, 29 Nov 2012

November 29, 2012: Over the last few years the U.S. Army has been increasingly effective in blunting the flood of pro-terrorist propaganda via the web and other media. The main method is to set up foreign language web sites specializing in Islamic terrorism or Islamic radicalism and then just report the truth. This also works with radio stations and the U.S. Army Special Forces have long used this technique. The Internet has the advantage of reaching a worldwide audience and is a lot cheaper to operate than radio or TV stations.

While there is some criticism of these military efforts to counter pro-terrorist propaganda, it's not as bad as the heat the military takes when it pays journalists to write pro-American stories for web sites that are read by many in Moslem countries. This sort of thing is always controversial in the United States, but during the Cold War the communists bought foreign journalists on a large scale. It wasn't hard to do, as in most parts of the world reporters regularly take money from people who want a more favorable story. Actually, this practice goes back to the beginning of modern journalism two centuries ago. The concept of independent reporting is largely an American one. However, in the United States, favorable media coverage is still bought. It's just that cash is rarely used. Publicists and spin masters trade favors and influence to get the stories they want.

In wartime, manipulating the media is considered just another desperate measure necessary to win the battle and save American lives. The problem with the war on terror is that it is a rather more murky conflict. Although Islamic terrorists pulled off a "Pearl Harbor" in the form of the September 11, 2001 attacks, and are every bit as cruel and murderous as the World War II Nazis and Japanese, there are many Americans who disagree on what tactics are permissible for fighting this war. Moreover, this is not the 1940s. Times, and attitudes, have changed. But bribing journalists, in parts of the world where the enemy is doing it, is more self-defense than anything else. If you don't do it, you just put more Americans at risk. Thus defending such practices becomes yet another battle in the war on terror.

The military quickly found it was more effective just to set up new websites and get out a more accurate message. Islamic terrorists rely a lot on fantasies and lies. Their message can't handle the truth and Westerners are surprised to see what kind of twisted versions of reality are posted on pro-terrorist web sites. While the hard core terrorist fans are not swayed by the truth, many potential recruits are. While terrorists love to show videos of soldiers and police being attacked, they are very unhappy if someone shows the more usual reality; dead women and children who were hurt by the many terrorist attacks that don't work as intended. Another key advantage of running your own sites is that you don't expose anti-terrorist journalists. Islamic terrorists are quite fond of kidnapping, torturing and killing journalists who oppose them.

Table of Contents

10th Annual Army Global Information Operations Conference

We have entered the planning window for the 10th Annual Army Global Information Operations Conference hosted by the SMDC/ARSTRAT G39 at Peterson Air Force Base Colorado. The conference is scheduled for 15-19 April 2013. Our proposed theme this year is "Information Operations from Steady State to Crisis". This addresses a changing landscape in military information operations that can rapidly escalate, and how we posture ourselves to adapt.

We intend to conduct work groups again this year and refine that process some more, and are soliciting ideas for topics and volunteers to facilitate these work group discussions. Some proposed work group topics are: Non-traditional Assessment; Cyberspace as an IIA medium; IIA Professional Development Opportunities.

More information will be provided later once we complete the approval process. Points of contact are Scott Janzen scott.c.janzen.civ@mail.mil, 719-554-8890; or Jose Carrington, jose.carrington.civ@mail.mil, 719-554-8880.

Table of Contents