Information Operations Newsletter

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

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

ARSTRAT IO Newsletter Online

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

Table of Contents

Vol. 13, no. 07 (May 2013)

Social Banditry and the Public Persona of Joaquín "El Chapo" Guzmán - Implications for Information Operations in Guatemala

By Guy Fricano, Small Wars Journal, Apr 29 2013

Abstract: This article reviews nine key insights into social banditry originally described by Eric Hobsbawm and examines their applicability regarding Joaquín "El Chapo" Guzmán, leader of Mexico's Sinaloa Cartel. Because some of Mexico's organized crime leaders aim to be viewed as social bandits, and visit Guatemala and the Mexico-Guatemala border region to evade authorities, the article focuses on particularities of those culture zones in the potential application of three primary strategies of information operations to contest a social bandit's prestige: emphasizing distance between the social bandit and the local poor, portraying collusion of the social bandit with local authorities and opposition to federal authorities, and emphasizing closeness between federal power and the local poor. A criminal organization leader who desires the prestige of social banditry would have cause to oppose each strategy. The analysis predicts that the first two strategies are more realistic, potentially more important strategically, and are more likely to become intensely contested through Information Operations, within culture areas of Guatemala and the Mexico-Guatemala border region.

Joaquín Archivaldo Guzmán Loera, alias "El Chapo"

In late February 2013, multiple reports originating in Guatemalan, Mexican, and American news media claimed that Sinaloa Cartel leader Joaquín Guzmán, alias "El Chapo", was killed in a shootout near the Mexico-Guatemala border. This turned out to be the latest of numerous false reports of his capture or death.[1] It appears Guzmán is alive and his power remains unparalleled within Mexico's Drug War.[2]

The nature of that power is distinctive in its magnitude, as well as the prestige associated with his persona.[3] In terms of magnitude, he has far surpassed Al Capone and Pablo Escobar to become the most powerful crime lord in history.[4] In this sense, his influence is rivaled primarily by Miguel Treviño (alias, "Z-40"), leader of Los Zetas, the most powerful transnational criminal organization opposing Guzmán's Sinaloa Cartel. However, Guzmán's prestige is distinguishable from that of any other Mexican crime lord in the extent to which his persona is perceived as a heroic champion of Mexico's poor. Conversely, Treviño is widely viewed as a sadistic narco-terrorist. The difference in public perception is striking because Guzmán and the Sinaloa Cartel draw upon the same methods that have blackened the reputation of Treviño and Los Zetas, including bribery, murder, torture, terror tactics, and targeting of enemies' families.

The Importance of Information Operations in Mexico's Drug War

It has been claimed that some of Mexico's organized criminals use information operations to manage their public images as social bandits (to be discussed shortly), and that Joaquín "El Chapo" Guzmán has been particularly successful in that regard.[5] The position taken here is that the comparison of Guzmán's prestige to social banditry is valid, and additionally, that the perception of social banditry has not been perfectly established. While commonalities between Guzmán's persona and that of the social bandit are important, notable divergences also exist. Taken together, these represent key issues around which his valorized persona is, or may be, contested. A systematic, though necessarily brief, comparison between them will illuminate implications regarding information operations for and against the Guzmán and the Sinaloa Cartel. Finally, the article will emphasize how peculiarities of the Mexico-Guatemala border region, where Guzmán is believed to visit frequently,[6] [7] may inflect information operations in those culture areas.

There exists a paradox when a crime lord such as Joaquín Guzmán (whose heroism is more likely to be acknowledged in Western Mexico) approaches the Mexico-Guatemala border. His ability to evade capture from either Mexican or Guatemalan authorities is augmented, while his prestige is comparatively diminished among local populations. Additionally, arch-rivals Los Zetas are more deeply entrenched in Guatemala and the border region. The paradox can be resolved through many possible outcomes, including Guzmán's persona achieving increased prestige in or near Guatemala, his persona becoming demonized in that region, the Sinaloa Cartel eclipsing Los Zetas as Guatemala's dominant criminal organization, or his leaving Guatemala and the border region by will, capture, or death. As several of these possibilities can be facilitated or complicated with carefully conceived information operations, it will become especially important to consider how this could develop should such a campaign intensify within Guatemala.

Social Banditry

Social Banditry is distinguishable from other forms of banditry by a perceived relationship between the bandit (and his organization) with those who are socially (and often geographically) distant from state power. It symbolizes a special type of protest and rebellion on behalf of the impoverished peasantry.[8] Unlike typical banditry, robbery of the social bandit becomes interpreted by admirers as contributing to the redistribution of

wealth to those who have been unjustly impoverished.[9] The social bandit's killing, theft, and other forms of criminality are not directed toward the peasantry, with whom he identifies and comes to represent symbolically through using tools available to them (including strength, bravery, cunning, and determination) to expropriate in the service of a superordinate cause in the people's interest.[10] Social banditry can be found in practically any society with disenfranchised peasantry. English-speakers are most familiar with it through the mythology of Robin Hood. Mexico's extensive tradition of social banditry has produced national heroes such as Pancho Villa, fictional heroes such as Zorro, and religious icons such as the narco-saint Jesus Malverde, whose cult is loosely affiliated with the Sinaloa Cartel.[11]

Eric Hobsbawm[12] has identified nine key aspects of a noble robber's public image (as opposed to the true man) regarding his relations with the peasants who aspire for solidarity and identity. While Joaquín Guzmán is regarded by some Mexicans as usurping from the rich to give to the poor, he is envisioned more specifically as a cunning, ruthless, specifically Mexican international criminal entrepreneur who creates jobs for the poor and distributes considerable bribes to the rich while usurping from criminal rivals. Nonetheless, the observation that crime lords such as Guzmán attempt to bolster their public images with the prestige of social banditry has merit. To the extent that Guzmán wishes to consolidate the benefits of association with the romanticism of social banditry, and to the extent to which Mexican or Guatemalan state authorities and criminal rivals intend to prevent this, Hobsbawm's key observations offer a framework to highlight essential aspects of Guzmán's persona likely to be contested between the Sinaloa Cartel and Guzmán's enemies within Guatemala and the Mexico-Guatemala border region. These implications may also be relevant in other Central American nations, particularly Belize, Honduras, El Salvador, and Nicaragua, where the Sinaloa Cartel and Los Zetas are expanding to compete for impunity in drug production and trafficking, weapons trafficking, human smuggling, kidnapping, extortion, prostitution, murder-for-hire, petroleum theft, money laundering, and other sources of profit-generation.

1.The Social Bandit's career begins as a victim of injustice, or persecution by authorities for acts that they, though not the local people, view as criminal. Guzmán's origin is widely seen within Mexico as a rags to riches story originating in Mexico's Sierra Madres, a region known for its lawlessness, as well as its capacity for drug production and distribution. While Mexican and U.S. authorities may consider those drugs illegal, desperately poor local populations do not share the sentiment. That Guzmán is regarded as achieving tremendous wealth and power through a business that is illegal according to federal and state authorities but sanctioned according to local norms works in his favor in Western Mexico. Guatemala needs the job creation his organization would bring, but remains more ambivalent about drug trade due to escalating patterns of addiction in local populations.

2.The Social Bandit rights wrongs. Even within Mexico, Guzmán is perceived as driven more by expansionistic ambition and revenge than a desire to right wrongs. However, enemy operatives (as well as his own) are frequently vicious and sociopathic even when not following orders. The Sinaloa Cartel's previous efforts to frame violence against enemies as retaliatory justice have been intermittent, and without the consistency required for effective message communication. The potential to consolidate his image through more consistent applications of this strategy is far from exhausted in Western Mexico. Many Guatemalans are willing prospects for employment from a Mexican criminal organization, although they (like most Central Americans) would not expect any Mexican power-broker to right wrongs against them in Mexico, much less in their nations of origin.

3.The Social Bandit takes from the rich to give to the poor. This generality is most applicable to Guzmán's ability to provide jobs to poverty-stricken Mexicans through lucrative drug trade with self-destructive gringos (sometimes construed within Mexico's popular imagination as "the rich"). Trade, however, is quite different from the cause-driven expropriation typical of social banditry. Another complication is Guzmán's infamous readiness to spend vast sums of money upon bribes – the larger amounts typically going to those who wield state power, including many who are already wealthy. Poverty is even worse in Guatemala, where job creation may inspire a blind eye to the unsavory aspects of his organization. Again, Guzmán has not yet mounted a sustained campaign to convince average Guatemalans why the Sinaloa Cartel's presence should be welcomed. Like in Mexico, the strategy of portraying oneself as taking from the rich and giving to Guatemala has yet to be fully exploited or discredited. Given the certainty of Guzmán's money invigorating local economies, it is likely to become a point of greater contention.

4.The Social Bandit never kills except in self-defense or just revenge. Within Mexico, Guzmán has a well known history of aggressing against former allies, including the Arellano-Félix Organization, the Juarez Cartel, and the Beltrán-LeyvaOrganization. Los Zetas have accused him of opportunistically breaking non-aggression pacts. He is not typically regarded as killing only in cases of self-defense or just revenge. Though many drug war killings could potentially be framed as self-defensive or retaliatory in some sense, the Sinaloa Cartel has attempted this only intermittently. Even on occasions when Guzmán's own children have been murdered, the

Sinaloa Cartel has not responded with concerted efforts to garner the public's support to legitimize violence, though it would have been accepted by most fathers as a sensible motive for lethal retaliation. In Mexico or Guatemala, the Sinaloa Cartel would need to consistently and convincingly communicate extenuating circumstances to local populations to reverse that trend.

5.The Social Bandit returns to his community as an honored citizen. In a certain sense he never leaves the community. This depends upon which community is the point of reference. It is more valid within Western Mexico, particularly in Sinaloa, where Guzmán's power is based. It is not equally true along the gulf coast of Mexico, which is dominated by Los Zetas (an enemy organization) or the Gulf Cartel (a previous enemy and presently a tentative ally against Los Zetas). It is less valid in Central America, where local populations frequently experience discrimination and exploitation as migrants in Mexico. Notably, Guzmán has not always been welcomed as an honored citizen in Guatemala, where he was arrested in 1993.[13] While Guzmán may still be an honored citizen in some areas of Western Mexico, he would need to win over local Central American populations ready to perceive him as a Mexican land-owner – a social type typically presumed guilty until proven innocent of exploiting migrants from their societies.

6.The Social Bandit is admired, helped, and supported by his people. Again, this is truer in Western Mexico, where his power-base is most secure. It is less true along the gulf coast or in Southern Mexico, where his safety is more dependent upon bribery, weapons, the integrity of his networks, and the quality of his operatives. Its applicability is more doubtful in Central America. The loyalty of Guatemalans to the Sinaloa Cartel is due almost entirely to a combination of their terror and his willingness to employ, bribe, and share profits, and not because he is perceived as a beloved champion of the people. Los Zetas have traditionally recruited more extensively than the Sinaloa Cartel from Guatemala, resulting in better connections among local authorities and criminal groups. While this makes it less likely for local populations to assist him out of sympathy, closer associations between Los Zetas and locally detested state authorities and criminals could be exploited to the Sinaloa Cartel's favor.

7.The Social Bandit dies invariably through treason because no decent member of the community would act against him. To date, Guzmán has used lethal violence and extraordinary cruelty against suspected betrayers, and on some occasions, their relatives. This has not typically corresponded with attempts to frame his enemies as indecent members of the community. In fact, there have been several occasions where former criminal partners or subordinates have acted against Guzmán after accusing him of betrayal, including members of the Arellano- Félix Organization (previously the Tijuana Cartel), the Beltrán-Leyvabrothers (who broke away to form a rival cartel), and certain operatives of Ignacio Coronel Villarreal (some of whom went on to establish the New Generation Cartel of Jalisco following his death). Guatemalans are more likely to be dissuaded from acting against the Sinaloa Cartel through bribery and terrorization than from the perception that anyone who acts against him is an indecent member of the local community. In Guatemala, as in Mexico, it doesn't require much imagination to frame criminal rivals as indecent persons. This is another strategy that has yet to be further developed by Guzmán and his enemies. It is notable that Guatemalans have acted against him previously, such as when he was arrested there in 1993.

8.The Social Bandit is invisible and invulnerable. The appearance of invulnerability against state and criminal enemies is an important component of his persona. Ongoing evasion from capture or death has demonstrated cleverness, resolve, and power that many find suggestive of de facto invulnerability. Invisibility is more disputable. His famed elusiveness is cast in relief against tales of public appearances, where enforcers confiscated telephones from all other patrons at restaurants while he ate, then paid their tabs upon his departure. Regardless of their veracity, most or all of such accounts supposedly took place in Mexico. The author is not aware of similar public displays of magnanimity in Guatemala. Another exception to invisibility was an interrogation disseminated in 2012 through social media[14] in which a man who resembles Guzmán gruffly interrogates a bound captive about enemy movements.[15] It is unknown where the interrogation took place. Guzmán's most famed public appearance in Guatemala was against his will, when he was photographed in a trophy-like media event following his arrest there in 1993. However, his successful escape from prison in 2001 continues to bolster the image of de facto invulnerability.

9.The Social Bandit is not the enemy of the king or emperor (the font of justice), but only against detested gentry, clergy, or other local authorities oppressing the poor and powerless. Guzmán's power base requires, and has benefited from, his success corrupting and controlling the Mexican state and municipal authorities or killing those who cannot be manipulated. Municipal authorities he struggles to control (e.g., the Juarez police; the Tijuana police) tend to be those well infiltrated by other criminal organizations. His power is too great to be rivaled by any local landowner, clergy, or corrupt politician. In Mexico, only federal authorities have the resources needed to challenge the Sinaloa Cartel. Despite claims by Mexican authorities suggesting his capture is their top priority,[16] the Sinaloa Cartel may have infiltrated Mexico's federal police and military

more effectively than any other organization. Whether by infiltration, terrorization, or simply considered the lesser of two evils, it is widely speculated throughout Mexico that Mexican (and US) federal authorities do not pursue the Sinaloa Cartel with the same resolve as its arch-rivals Los Zetas. Nevertheless, this has not prevented Guzmán from publically accusing Mexican authorities of complicity with Los Zetas.[17] Such claims are impossible to prove, but at face value would appear credible to Mexicans who generally expect corruption and injustice from federal leadership. The situation is different in Guatemala, where Los Zetas probably have infiltrated Guatemalan state and municipal authorities more effectively than has the Sinaloa Cartel. To the extent the Guatemalan public sees their authorities as wielded by Los Zetas, there exists an opportunity for Guzmán to present himself as opposing local oppressors. The dissemination of claims such as Los Zetas slaughtering Central American migrants,[18] throwing them from moving trains for not paying tariffs,[19] and threatening a priest with death for speaking out against such abuses toward migrants,[20] [21] suggests the Sinaloa Cartel is exploring this strategy. Only consistent efforts over time will reveal its full potential for or against Guzmán in Guatemala.

Implications for Information Operations in Guatemala and the Mexico-Guatemala Border Region

The dependence of social banditry upon a specific geographic region, populace, and pattern of relations with state power yields three fundamental strategies through which that particular prestige of Guzmán's public persona may be contested in Guatemala, or near the Mexico-Guatemala border.

Distance between the Social Bandit and the Common Poor

The first strategy is to emphasize distance between the social bandit and the common people, particularly the poor. This will likely become the most important domain of contention because of the possibility for Guzmán to mount a coherent plea to poverty-stricken Central Americans. Philanthropy is an important factor that separates a social bandit from other robbers and murderers. Like most Mexican crime lords, Guzmán almost certainly donates to local causes, including schools, parks, and social programs. He would merely need to make such information more clearly understood by the local population. State authorities can do little against this approach if the funding required for such services is unavailable from legitimate sources. An alternative would be to counter-balance images of philanthropy through disseminating verifiable incidents of the poor suffering within his sphere of influence. Unfortunately, not even Guzmán can solve Guatemala's problems, and there will be greater potential for this counter-response on behalf of Mexican or Guatemalan authorities, or Los Zetas, none of whom want the Sinaloa Cartel further entrenched in Guatemala. Guzmán can and probably will use this strategy against Los Zetas[22] by continuing to disseminate stories of oppression, exploitation, extortion, rape, and murder of the local poor at their hands.

The fact that Guzmán wields considerable financial and geopolitical power makes his persona potentially vulnerable to apparent vigilantism and peasant rebellion against him. Repetitive and credible reports of social bandits rebelling against his own power, and eluding his efforts to control their homelands, could work in the favor of such results.

Another potential threat comes from the current trend of communal autodefense, whereby ostensibly normal Mexican citizenry are banding to combat organized criminals who are degrading public life. While some of these groups are sincere, there is cause to believe that many have been infiltrated (or even created) by those very organizations. One recent mass arrest resulted in accusations of a community group being infiltrated by the New Generation Cartel of Jalisco,[23] which recently broke its alliance with the Sinaloa Cartel. Similar mass arrests have resulted in accusations against the Knights Templar cartel.[24] It is likely other cartels (including the Sinaloa Cartel) also have infiltrated these groups as part of their ongoing effort to protect their own impunity and imperil their criminal rivals. Much of the propaganda that has been disseminated thus far under the ostensible guise of communal autodefense will not be effective against Guzmán or the Sinaloa Cartel because the persons who have been captured and "tried" at those public proceedings typically were accused and addressed as predacious individuals – that is, kidnappers, extortionists, rapists, killers, etc., rather than faithful operatives of a predacious organization or leader.

Closeness between State Power and the Common Poor

The second strategy that could potentially be used to counter a social bandit's prestige would be to emphasize closeness between state power and its people, particularly the common poor. In the case of Guatemala, however, this approach is less realistic due to intense suspicion toward government corruption and ineptitude. Corruption may be worse in Guatemala than in Mexico, and Guatemalans may be more distrustful than Mexicans of their own state authorities. Guzmán would have the advantage here, as the Sinaloa Cartel merely needs to continually remind Guatemalans of what they already believe – that the authorities they normally distrust are now aligned with Los Zetas.

Collusion with Local Authorities and Opposition against State Authorities

The third strategy to counter a social bandit's prestige is to emphasize his collusion with (corrupt) local authorities and his opposition against (just) state authorities. There would be little Guzmán could do to discredit stories of collusion with local authorities, as they would be received uncritically by Guatemalan consumers. As an alternative, Guzmán's counter-strategy may be to disseminate news of his opposing corrupt local authorities wielded by Los Zetas. Although Guatemalans generally do not perceive their federal authorities as just, Guzmán will seek to avoid appearing as a threat to Guatemalan sovereignty. This will require effort, as a gangster's relationship with the local political power structure is usually more evident than in the case of the traditional, rural social bandit.[25]

Summary and Conclusions

As Joaquín "El Chapo" Guzmán and other crime lords increasingly rely upon the Mexico-Guatemala border region to evade authorities, information operations will need to be adjusted by state authorities attempting to influence public reaction to such figures, or by criminals seeking to alienate the public from one another. A systematic theoretical examination of social banditry yielded three primary strategies along which an individual's prestige as a social bandit may be refuted (or protected). These include emphasizing closeness between state power and the local poor (a difficult prospect in Guatemala), emphasizing the social bandit's collusion with local authorities and opposition to state authorities (a more realistic prospect), and emphasizing distance between the social bandit and the common poor (predicted as the most important of the three within Guatemala). To enhance his prestige as that of a social bandit near or within Guatemala, Guzmán's essential strategies would be to emphasize distance between state power and the local population (especially the poor), emphasize opposition against local authorities wielded by rivals Los Zetas, avoiding direct opposition to Guatemalan state authorities, explaining how his presence invigorates the local economy, and publicizing local philanthropy. State-sponsored information operations campaigns that do not make the above described adjustments to account for these primary strategies will not yield ideal results in Guatemala or the Mexico-Guatemala border region.

Notes:

[1] "5 falsas capturas de 'El Chapo'". Tierra del Narco. Feb 5, 2013. Accessed March 10, 2013: http://www.tierradelnarco.com/2013/02/5-falsas-capturas-de-el-chapo.html

[2] Hernandez, Anabel. ""El Chapo" reestructura y expande su imperio". Proceso. Feb 23, 2013. Accessed March 10, 2013: http://hemeroteca.proceso.com.mx/?page_id=278958&a51dc26366d99bb5fa29cea4747565fec=334426

[3] In this article, persona refers to a public perception (accurate or inaccurate) of personhood, as distinguished from personality, which would refer to essential aspects of personhood that remain continuous between different social contexts – regardless of the perceptions of others. Empirically-based metrics of persona may not necessarily correlate with metrics of personality.

[4] "El Chapo Guzmán más peligroso que Al Capone para EU". Tierra del Narco. February 2013. Accessed March 10, 2013: http://www.tierradelnarco.com/2013/02/video-el-chapo-guzman-mas-peligroso-que.html

[5] Sullivan, John P. "Criminal Insurgency: Narcocultura, Social Banditry, and Information Operations". Small Wars Journal. Dec 3, 2012. Accessed March 10, 2013: http://smallwarsjournal.com/jrnl/art/criminal-insurgency-narcocultura-social-banditry-and-information-operations

[6] "El "Chapo Guzmán" se oculta en El Petén, Guatemala". Notinfomex. Feb 7, 2013. Accessed March 10, 2013: http://www.notinfomex.info/2013/02/el-chapo-guzman-se-oculta-en-el-peten.html

[7] Carrasco Araizaga, Jorge. "El Chapo, también protegido en Guatemala". Proceso. June 6, 2011. http://www.proceso.com.mx/?p=271950

[8] Hobsbawm, Eric (2000). Bandits. Revised Edition. The New Press. 45.

[9] Hobsbawm, 95.

[10] Hobsbawm, 95, 121-123.

[11] Sullivan, John P. "Criminal Insurgency: Narcocultura, Social Banditry, and Information Operations". Small Wars Journal. Dec 3, 2012. Accessed March 10, 2013: http://smallwarsjournal.com/jrnl/art/criminal-insurgency-narcocultura-social-banditry-and-information-operations

[12] Hobsbawm, Eric (2000). Bandits. Revised Edition. The New Press.

[13] Carrasco Araizaga, Jorge. "El Chapo, también protegido en Guatemala". Proceso. June 6, 2011. http://www.proceso.com.mx/?p=271950

[14] "Difunde blog del narco supuesto video de "El Chapo"". Proceso. March 12, 2012. Accessed March 10, 2013: http://www.proceso.com.mx/?p=300773

[15] It is unclear how old the video was when it was disseminated in March 2012. It was a 1 minute 44 second portion of a longer, unreleased interrogation. Additionally, the figure resembling Guzman does not acknowledge the camera, and it is uncertain whether he was aware of the recording.

[16] "Es 'El Chapo' principal objetivo del gobierno mexicano: Segob". Historias del Narco. Feb 15, 2013. Accessed March 10, 2013: http://www.historiasdelnarco.com/2013/02/es-el-chapo-principal-objetivo-del.html

[17] "Narcocomunicado de El Chapo Guzman para el Z40...". Mundo Narco. February 12, 2013: Accessed March 10, 2013: http://www.mund0narco.com/2013/02/narcomensaje-de-el-chapo-guzman-para-el.html

[18] "¿Mataron Los Zetas a cientos de migrantes en Chiapas?". Mundo Narco. September 24, 2012. Accessed March 10, 2013: http://www.mund0narco.com/2012/09/mataron-los-zetas-cientos-de-migrantes.html

[19] "Zetas arrojan a migrantes de tren en movimiento si no pagan la cuota ". February 25, 2013. Mundo Narco. Accessed March 10, 2013: http://www.mund0narco.com/2013/02/video-zetas-arrojan-migrantes-de-tren.html

[20] "Sacerdote que ayuda a migrantes no se deja intimidar por amenazas de muerte de Los Zetas". Mundo Narco. August 12, 2012. Accessed March 10, 2013: http://www.mund0narco.com/2012/08/sacerdote-que-ayuda-migrantes-no-se.html

[21] "¿Amenazaron los Zetas con matar a un sacerdote que ayuda a los migrantes pobres?". Mundo Narco. June 8, 2012. Accessed March 10, 2013: http://www.mund0narco.com/2012/06/amenazaron-los-zetas-con-matar-un.html

[22] Because Los Zetas have established more connections in Guatemala, and Zetas' leader Miguel Treviño is not perceived as a social bandit anywhere (nor has he publically indicated interest in managing his public image in such a manner), it is more likely Guzman's information operations near and within Guatemala will attempt to demonize the Los Zetas organization more than Treviño's person.

[23] “Caen 30 miembros del cártel de Jalisco infiltrados en la policía comunitaria”. Mundo Narco. March 7, 2013. Accessed March 10, 2013: http://www.mund0narco.com/2013/03/caen-30-miembros-del-cartel-de-jalisco.html

[24] “Detienen a otros 17 miembros de grupo de autodefensa en Michoacán”. Proceso. March 11, 2013. Accessed March 11, 2013: http://www.proceso.com.mx/?p=335981

[25] Hobsbawm, 96.

Table of Contents

India Sets Up Social Media Monitoring Lab

By Nitin Puri for Mobile India, March 19, 2013

A specially-trained team of 20 police officers will staff The Social Media Lab and will work around the clock to keep an eye on issues being publicly discussed and track matters relating to public order. The intent behind the Social Media Lab is to assess changes in mass moods that could lead to gatherings and or possible protests on a large scale.

The Social Media Lab, inaugurated on Saturday by Bollywood actor Abhishek Bachchan, will gauge the mood of people on social media. They will also follow active netizens on Twitter, Facebook, Google+ and other social networks.

In other words, police will keep a close watch on Internet activists.

In November, Mumbai Police sparked outrage and fierce debate about India's Internet laws by arresting two young women over a Facebook post criticizing the shutdown of Mumbai after the death of a local hardline politician. The case also included several arrests across India for political cartoons or comments made online.

Naturally, this raises the question of the freedom of expression and the rights of Indian citizens. However, the average social media user shouldn't change their online behavior and habits, as this monitoring is not related to censorship. After all, the intent of the Social Media Lab is to prevent demonstrations and protests which can not only cripple a city, but the entire country.

Furthermore, most police departments across India, such as Delhi Police, already have dedicated cybercells and are active in maintaining law and order. For example, Delhi Police is active on Facebook and Twitter, by not only reaching to social media users for tips for crimes, but also by providing real-time traffic updates.

If social media users look at the positive versus the negative and embrace online monitoring, it's for their own good.

Another way to look at this is to realize and understand the millions of youth within India who are already active on social media. Some form of moderation and monitoring is in fact required, especially at an early age, to deter users from falling into the pitfalls of online bullying or even cybercrimes itself.

That being said, while the argument of freedom of expression will always be debated regarding online monitoring, social media users should also realize that real-time monitoring of posts and updates are just another way of being safe and secure, both online and offline. Media tends to only report the how online policing results in the arrests or detainment of others, when in fact, it can and has already been used for the safety and security purposes of both people and their communities within India.

According to social media experts, the amount of data covered by posts, updates, and tweets, will be next to impossible to monitor. Instead the department can single out netizens with criminal records, anti-social and anti-national agendas and track their online activities.

Table of Contents

Hacking the News: Information Warfare in the Age of Twitter

By Mandy Nagy, Legal Insurrection, May 1, 2013

The group of pro-Assad hackers calling itself the Syrian Electronic Army hacked The Guardian news outlet over the weekend, marking the latest in a string of cyberattacks from the same organization. The incident emphasizes the potential threat such attacks could pose if executed for goals far more malicious than intimidation or mere gain of public attention. And news outlets are among the most useful targets to such groups.

The attack on The Guardian was in apparent retaliation for the outlet’s coverage on the conflict in Syria. Last year, The Guardian also published a cache of emails between Syrian president Bashar al-Assad and his inner circle, in articles that were, not surprisingly, not very flattering of Assad.

On April 15th, the same organization hacked NPR and several of its Twitter accounts, also over the outlet’s coverage of Syria. Only days later, the Syrian Electronic Army hacked several of CBS’ Twitter accounts and sent out pro-Syrian propaganda, including false claims that the CIA is arming Al-Qaeda terrorists in Syria.

The same week, the group also compromised Twitter accounts of the Associated Press to tweet out a false message, causing the Dow to temporarily plummet.

The false tweet said there had been two explosions at the White House and that President Barack Obama was injured. The attack on AP's Twitter account and the AP Mobile Twitter account was preceded by phishing attempts on AP's corporate network. […]

The false tweet went out shortly after 1 p.m. and briefly sent the Dow Jones industrial average sharply lower. The Dow fell 143 points, from 14,697 to 14,554, after the fake Twitter posting, and then quickly recovered.

And in March, several of BBC's Twitter accounts were also hacked by the same group. They tweeted out snarky messages such as, "Saudi weather station down due to head-on collision with camel."

But these attacks from the Syrian Electronic Army aren't limited to recent weeks.

In August of 2012, they broke into the blogging platform and Twitter account of Reuters news service. A series of tweets followed, touting "heavy losses" in the Free Syrian Army, one of the anti-Assad rebel groups in Syria, and other pro-Assad messages.

In April of 2012, they hacked the Al-Arabiya news network. During that incident, the hackers disseminated messages that "the Gulf Emirates Prime Minister and Foreign Minister had been relieved of his duties and replaced by the country's heir-apparent," followed by a message about "an explosion at a Qatari natural gas field which killed dozens of people." The pace at which that news spread was dangerously quick. It caused many to fear a rift within the Qatari Royal Family – had the fake news not been refuted as quickly as it was, chaos could easily have followed.

Some suspect that the Syrian Electronic Army may actually be an army of one. Others suspect multiple hackers are involved. Either way, the threat is real.

I've covered the Syrian Electronic Army for over a year, as well as other hacker organizations, and have observed a significant uptick over time in the attacks by way of social media, notably on such useful targets as news outlets. Information warfare has become a legitimate danger in spreading propaganda in this day and age, especially in light of various conflicts around the world.

This weekend's attack on yet another news agency only highlights the dangers we face in these days of information warfare. While hacking attacks certainly present problems and can compromise crucial systems, the hackers' dissemination of disinformation and propaganda can be just as dangerous in the midst of such a hostile global conflict where information influences the decisions and acts of so many, including anyone from rebels on the ground to leaders of allied and opposing governments.

Twitter is fast becoming the weapon of choice in such cyberattacks. As we've seen, hackers succeeded in temporarily plunging the stock market with one false tweet from a reputable news outlet. Overseas in Qatar, they very well could have succeeded in creating chaos and panic. What lies on the horizon?

While the Syrian Electronic Army's objectives thus far have been focused primarily on generating publicity, these incidents should serve as a warning of the damage that could be done by hackers with a more strategic and aggressive goal in mind.

Table of Contents

Information Operations Is Just another Media Format Vying For the Eyes of the Audience

Contributor: The Platform, posted on DefenceIQ, 04/10/2013

The following article has been written by a senior producer/director and Information Operations specialist at The Platform, a neutral strategic communications, media services and information management business working in stressed territories around the world.

_____

"You can design and create, and build the most wonderful place in the world. But it takes people to make the dream a reality" - Walt Disney.

As far as I know, Walt Disney isn't often cited in articles about information operations, but, having borrowed the anthem of the Seven Dwarves for the title of my article, it seemed but a short hop to allude to the sentiments of their creator. However, there's editorial method in the madness.

Politicians, soldiers, strategists, advertising agencies and PR men are all adept at conjuring compelling visions of utopia – or at least peace and prosperity – for afflicted societies. But, as Walt Disney said, 'it takes people to make the dream a reality'. Beyond the world of cartoons and magic kingdoms, the same is true. Ordinary

people are the real agents of change, and information operations are intended to help inform, influence and inspire those people toward making the decisions and adopting the behaviours that ensure the dream becomes a reality.

To talk of 'dreams' may imply something fantastical or ostentatious, but in the stressed territories where information operations are often applied, people's dreams are surprisingly modest: peace, security, a job, a future. Very few people in the world do not share this basic suite of ambitions, and information operations can exert great emotional power when acting upon these desires.

My interest in influence operations is as a practitioner. However, I'm not a soldier, civil servant or academic, though I've worked alongside all of those groups. I'm part of a small coterie of professional people whose impact upon information operations is often taken for granted, but whose direct influence is out of all proportion to their number and status.

As a television producer/director, I and my colleagues interpret strategic intent and bring it to life. Without producers, directors, editors, cameramen and sound recordists, the campaigns and strategies, however eloquently described and however persuasively sold, remain confined to the gaudy realm of the Powerpoint presentation. This is not to downplay the role of the strategist, campaign manager or anyone else, but simply to highlight the importance of the television maker's art in this field and to underline the point that upon the success or failure of the television product, may depend the success of the strategy. The product itself, whether it be a short news feature, a youth entertainment programme or a full blown documentary, is the vital nexus between target audience and strategy. If the product fails, so does the strategy, and so does the effort to influence.

The purpose of this article is to explore influence operations from the standpoint of the IO Producer, giving an insight into what he/she does, and explaining why the right people with the right skills and experience are critical to the overall success or failure of any information operation, and, moreover, are vital to the future of IO.

In this article I intend to convey my own experience, instinct and conviction as someone who not only worked in prime-time broadcast television for over a decade, but who, in the last five years of concentrated activity, has written, produced or presided over somewhere between 750 and perhaps as many as 1000 television influence products across various territories and various genres. I hope this piece will be a valuable summary of lessons learned from the recent past and offer some bold propositions for the future.

In writing this piece, I want to assert some of the principles I apply in creating IO products. I should say at the outset, 99% of my experience is in creating 'un-attributable' television products, and therefore the particular nuances of that field inform this article. My IO experience is in ENG (essentially, short news features), documentary and youth entertainment, amongst other formats. I was never concerned with television commercials, and I'm not going to talk about written material or radio, though some of the same principles may overlap.

I should also add, the bulk of this very concentrated experience is drawn from operations in Iraq, participating in an influence campaign that it's now rather fashionable to dismiss. Some of those who dismiss it are not perhaps acquainted with the intense daily activities of certain organisations, nor aware of the sophistication of some of the work or the innovation, let alone the products themselves. Whilse I certainly agree it's all up for serious review and I would still passionately critique the flaws that I critiqued while I was actually working in Iraq, I would be very cautious about promoting a wholesale dismissal of the advances made and the lessons learnt. Moreover, I would suggest the institutional knowledge gained in Iraq is invaluable.

In my opinion, there are some critical foundations to any IO product:

1. Firstly, whatever the message and whatever the intent, the product's primary challenge is to succeed as a piece of engaging and entertaining television. The clarity and persuasiveness of any strategic message contained in the piece is irredeemably compromised - if not totally lost - if the product doesn't grab the audience. Failure is assured just as certainly as if one scribbled a vital message and entrusted it to a dead carrier pigeon.

The role of the television professional is to capture the audience's attention and hold it, using all the skills of his craft. Not only does he interpret the strategy and breathe life into it, he provides the vital sugar that helps the medicine go down. This is why, in my opinion, you can't make successful IO unless you can make decent television.

2. IO products should aspire to compete with the best quality broadcast television, even if they are un-attributable.

I recognise that this assertion will seem counter-intuitive to some readers, because it's often contested that an un-attributable product should appear similar to locally produced programming in order not to appear conspicuous. That's often interpreted to mean it should look a little amateurish or home-spun. If the product is to deploy on social media and needs to look, 'user generated', that might be a consideration. However, I'd balance this concern about attribution - about products looking 'too good' - with a couple of thoughts.

Firstly, this notion has sometimes been employed cynically to excuse poor quality IO. That's not what the client pays for.

Further, it's folly to assume that all 'foreign telly' looks like Borat. It doesn't. Particularly in the Middle East, high-quality production values are appreciated and frequently seen (editorial or journalistic issues are another dimension, but let's confine ourselves to aesthetics for the time being). Secondly, to sustain the Middle East example, the demographic of the media industries there reflect the general demographics across the region. The Arab TV industry is young, comfortable with technology, multi-skilled, eager to learn and progressive. The TV industry in the Middle East is also influenced by the West - indeed a good many Western media professionals work in these industries now and standards are dramatically improving. Self-taught citizen journalists are moving into the mainstream media, being exposed to new technology and software, mastering it and seeking to excel. It would be complacent to assume that average work will continue to pass muster.

However, aside from professional pride, the overriding reason for making the best television we can possibly make, coincides with point one. It has to be judged at face value: It has to work as good television first. Bad or amateurish television doesn't suddenly 'work' because it's inconspicuous amongst the local programming. It simply means that it's not only bad television, it's bad IO too. My personal opinion is that if a product succeeds as a piece of television, the attribution will be of secondary relevance to the audience - it's the Trojan Horse effect. The audience is too busy consuming the narrative to consider where the message comes from. This is predicated, of course, on the assumption that the message is discreet, and based upon what is reasonable and logical, because though people might repudiate a message because of its assumed source, they can't generally repudiate logic forever.

3. Having talked quality, it's time to consider quantity, and this section assumes a broad, large-scale television campaign. The available funding and the capacity to carpet-bomb an audience with IO products might appear a desirable situation, but if the 'drumbeat' becomes a cacophony, problems emerge.

As a member of the IO community, and moreover, as someone with a mortgage, expressing this caveat might appear fatal to the fortunes of the industry. However, whilse volume might swell corporate coffers in the short term, increasing output in a given theatre of operations inevitably diminishes returns, particularly where one or two formats are relied upon disproportionately and become conspicuous.

Increased volume creates a necessity for increasing numbers of conduits. Products need to be deployed, and in most territories, there are a limited number of viable broadcasters that cater to the particular target audiences. Over time, and relative to the quality, quantity and subtlety of products, the major domestic broadcasters' desire to deploy material inevitably drops off. But, if the big boys won't play, smaller channels will.

Minor channels, devoid of serious audiences and consequently strapped for cash, will deploy IO products. Presumably, some of these minor channels exist only to deploy IO products. They become a conduit not only for ENGs, but for regular transfusions of life-giving IO Dollars. As deployment of IO products become the major revenue for the channel and more and more jostle for space on the same channels, so audiences drop off even further, and the IO deployed becomes increasingly worthless. In these circumstances, IO merely props up failing channels and distorts the market.

As a wry footnote to this proposition, I recall watching a selection of minor Iraqi channels in around 2009-2010. It was a somewhat bleak epiphany. One channel's output consisted almost entirely of back to back IO products, produced by various cells and exhibiting greater or lesser degrees of virtuosity. The IO products were interspersed with seemingly uncut footage of jubilant dancing sheikhs. I wondered at the time whether these frolicking Arabs might not have been the various channels' owners, convening to celebrate the latest dollar bonanza. I hasten to add, that is no slur on them.

As an émigré from broadcast television, it would seem obvious to me to ask how many people were seeing the IO products I was making – indeed, that became a bitter obsession for me in Iraq. Arguments were advanced that the wafer thin slivers of the audience pie that represented the viewership of a considerable swathe of IO (mainly ENGs), was justified as it represented 'key constituencies'. Above a certain threshold, there might have been some validity to this assertion. However, when certain broadcasters were offering a potential audience of 4% and less[1], it would have been a great deal cheaper to organise a key leader engagement and take enough baklava for everyone. Good products were the least that was being wasted.

In mainstream television, nothing matters more than eyeballs on the product. Given that reality TV ratings and sales of toothpaste are less important than many of the ideas being 'sold' in IO campaigns, we should be a similarly obsessed with audience numbers.

Fewer, higher quality programmes with a greater variety of formats, longer lead time and better deployment would, in my opinion, provide greater value for money, avoid saturation and reduce 'IO fatigue' amongst the audience. [2]

4. The ideal IO product is one that succeeds as an entertaining piece of regularly-broadcast media, securing its own following, and messaging effectively, but seemingly incidentally. It might be a youth orientated magazine programme, a historical documentary, or a news review, but it could equally be any other popular genre; it may be narrated or presenter lead: we're limited only by our skill and our creativity.

Experience tells me that all of the above formats are viable. However, by and large, ENGs are undoubtedly still the default option. I'll advance an alternative model below, but these are my thoughts on the IO workhorse.

ENGs have great utility from a number of points of view. Firstly, they should be relatively cheap to make, and it's possible to turn them round reasonably quickly. A few skilled editors and a similar number of experienced producers have been known to post-produce thirty plus high quality ENGs a month. However, as above, fewer products with greater opportunity to craft and refine, probably represents a better modus operandi. Frequently deployed in the commercial space - sometimes rather too abundantly for discretion – ENGs are still a powerful tool to influence attitudes and change behaviour, if correctly composed.

To work effectively, I believe ENGs should be produced with reference to the following considerations.

ENGs should reflect reality. The producers need, as far as is possible, to understand that reality. Ideally, they'd live amongst the people they're messaging and appreciate the challenges of daily life. Where that isn't possible, they have to make every effort to understand the social and cultural norms which colour the environment. This understanding must necessarily go a lot deeper than rote learning of superficial stereotypes. Producers shouldn't be afraid to acknowledge the negative; it builds credibility and authenticity, and conceding a skirmish might just help to win a messaging battle. Modest claims are better than bold claims, and less likely to backfire. Finally, manage expectations and never message on promises.

ENGs should relay the voice of the peoplenot the voice of the strategist. Sententious voiceover imposes a narrative, where the skillful television producer can draw out that same narrative from interviewees using carefully crafted journalistic questions. The best ENGs have minimal voiceover, or no voiceover at all, and speak to the audience in the familiar vernacular of everyday people - people to whom the audience can readily relate. This is a powerful means to convey a message.

Finally, stay journalistic, stay objective, stay in touch: don't IO yourself…

Being involved in a long term campaign, especially one where you are removed from the general populace and from life on the street, one's apt to start becoming susceptible to one's own messages. Read everything, watch as much domestic television as possible and consume social media. Products which don't reflect reality just don't work.

So, what's the future? This article isn't merely supposed to be a Bluffer's Guide to IO, it's intended to influence, believe it or not…

IO needs to change. In my opinion, it needs to become more like mainstream television. IO producers and their clients need to proceed from the same professional start point as their cousins in mainstream TV. They need to commence with the question, 'what do people want to watch?' Once they have answered that question, they can think about messaging. It doesn't mean the message is secondary, but simply that for the message to actually reach the audience, the vehicle has to be effective. This applies whether the product occupies the advertising space or otherwise. It cannot be taken for granted that people will watch. But we need to go further than making decent ENGs.

As global audiences become more and more segmented and people graze and multi-task even as they view, IO products will have to work much harder if they're to secure people's attention and perhaps even draw their own audiences. The best products will inform, some will entertain, some will even make people laugh. IO can be produced to exist within every media genre, and to some degree, it already has. It simply needs to be further refined. Moreover, clients need to fully understand what can be achieved by professional television makers. To that end, they need to talk to them directly, to gauge feasibility and cost from the outset of any project.

Considering all the many billions of dollars that have been spent on IO in the last decade, there has been surprisingly little innovation or audacity, and even less attempt to stand back and take a long hard look at the basic propositions upon which messaging is founded.

From my own perspective as an IO producer, my ambition is not to have to foist my products upon the audience, but to have the audience seek out those products. This can be achieved if they are first and foremost successful pieces of television, cleverly conceived and creatively composed. This might seem like a huge additional challenge for the IO community, but when viewed objectively it must be recognised that it's the only hope for IO, if it is to succeed in the multi-platform, multi-genre media world. The one thing consumers of media are not seeking out, is dull, worthy, unsubtle and amateurish film and television. So, unless you have a captive audience, what other options are there but to aspire to the standards and creativity of the mainstream popular media?

The answer to the above proposition might be, 'but that's not what we do!' My riposte would be, 'it needs to be'. Nobody will watch otherwise. A message can be woven into any vehicle, from a cookery show or reality format, to a full blown feature-length documentary. An experienced television producer/director will have spent their whole career following formats, composing narratives, adhering to editorial agendas - that's all 'messaging' is. And is the gulf between popular media and IO so wide? Let's look back.

In 1939, Jan Anstruther's fictionalised account of a wartime British family was published under the title, Mrs Minever. It recounted the tribulations of the eponymous heroine and her family as they braced for war, and subsequently fought it on the home front. The book crossed The Pond and became a huge publishing sensation at a time when America was still neutral, and the public, and many within the establishment, were still opposed to involvement in another European war. The book and the more famous film, which followed in 1942, was credited with engendering empathy for the beleaguered and embattled British, and having a significant influence on American attitudes toward joining the war. FDR credited the film with having hastened US intervention, while Churchill claimed it had been worth, 'six divisions'.

Different times? Well, perhaps. But what about Michael Moore or Morgan Spurlock? Don't they do IO? What about Richard Branson's latest documentary project, Breaking the Taboo, which comprehensively dismantles the strategy behind the war on drugs? Isn't that IO? And very compelling IO?

Admittedly the two documentaries, Fahrenheit 9/11 and Supersize Me, cost $6m and $1m respectively, but it's the ethic, not the budget and scale I'm highlighting here. These were engaging, entertaining narratives which sold complex ideas[3]. We're in the same game; we just have to play it better, using the right people. If there is any gulf between traditional IO and popular media in terms of influencing and motivating, it's only really in terms of relative success.

The point of the above illustration is not to advocate that the IO community goes head to head with Hollywood. But it's not far off. We at least have to see ourselves as competing in the same marketplace for the same audience. That's the critical point.

The ultimate expression of the above model will be a commercial satellite channel which generates its own audiences from a mixture of popular programming - some produced, some bought-in. The schedule would include subtle IO, and the overall editorial agenda would broadly suit the client or clients' needs. It may need to be populist, even tabloid in character, but what it can't be is dull. This model would see deployment issues become an irrelevance, and might even generate revenues. Audacious? Maybe. Possible? We believe so.

The challenge for the IO industry in coming years will be to draw people into it with the right skill set to realise a radical but necessary evolution. Principally, these people need to be experienced television professionals, not PR people, not ad men. Clients need to work closely with people who understand television, understand the possibilities and the constraints and, moreover, understand how you translate an idea directly into a piece of compelling television. A TV format or an editorial agenda is, after all, little different to a campaign strategy. Working directly with TV people from the outset of a campaign better enables clients to plan, assess and realise their goals.

The broadcast TV world has another unique selling point as far as IO and, more importantly, IO budgets are concerned. In the last ten years, as advertising revenues fluctuated and the market fragmented, production companies have had to do more with less. Long gone is the boozy TV lunch and the over-populated production team. The industry has become lean, versatile and efficient. Many good directors are also excellent cameramen; many producers write; many offline television editors can create from very average rushes a gloss and an allure that competes with costly TVCs.

The gold-rush years for IO have undoubtedly passed, at least for the foreseeable future. However, this provides an opportunity for sober reflection and recalibration. Clients need to know that much can still be

achieved. In my opinion, the skills, ethics and creativity of the television industry and its versatile professionals can serve the commissioners of IO well – and cost-effectively.

IO needs to be competing for its audience with the best broadcast television and online content. At the end of the day IO is just another media format vying for the eyes of the audience, and it needs to give itself the chance to compete. The industry needs the right people to engender a revolution.

Table of Contents

China's Cyberspies Outwit Model for Bond's Q

By Michael Riley and Ben Elgin, Bloomberg, May 2, 2013

Among defense contractors, QinetiQ North America (QQ/) is known for spy-world connections and an eye-popping product line. Its contributions to national security include secret satellites, drones, and software used by U.S. special forces in Afghanistan and the Middle East.

Former CIA Director George Tenet was a director of the company from 2006 to 2008 and former Pentagon spy chief Stephen Cambone headed a major division. Its U.K. parent was created as a spinoff of a government weapons laboratory that inspired Q's lab in Ian Fleming's James Bond thrillers, a connection QinetiQ (pronounced kin-EH-tic) still touts.

QinetiQ's espionage expertise didn't keep Chinese cyber- spies from outwitting the company. In a three-year operation, hackers linked to China's military infiltrated QinetiQ's computers and compromised most if not all of the company's research. At one point, they logged into the company's network by taking advantage of a security flaw identified months earlier and never fixed.

Graphic: Hackers in China Compromise U.S. Defense Secrets

"We found traces of the intruders in many of their divisions and across most of their product lines," said Christopher Day, until February a senior vice president for Verizon Communications Inc. (VZ)'s Terremark security division, which was hired twice by QinetiQ to investigate the break-ins. "There was virtually no place we looked where we didn't find them."

CyberPillage

QinetiQ was only one target in a broader cyberpillage. Beginning at least as early as 2007, Chinese computer spies raided the databanks of almost every major U.S. defense contractor and made off with some of the country's most closely guarded technological secrets, according to two former Pentagon officials who asked not to be named because damage assessments of the incidents remain classified.

As the White House moves to confront China over its theft of U.S. technology through hacking, policy makers are faced with the question of how much damage has already been done. During their multiyear assault on defense contractors, the spies stole several terabytes -- equal to hundreds of millions of pages --of documents and data on weapons programs, dwarfing in sheer quantity any theft of Cold War secrets. The QinetiQ hack may have compromised information vital to national security, such as the deployment and capabilities of the combat helicopter fleet.

"The line forms to the left when it comes to defense contractors that have been hacked," said James Lewis, a senior fellow in cybersecurity at the Center for Strategic and International Studies in Washington. "The damage has been significant."

Systems Hacked

A few of the attacks have become public, including the 2007 theft from Lockheed Martin Corp. (LMT) of technology related to the F- 35, the most advanced U.S. fighter jet. Intelligence officials say the damage is far more extensive than the limited public accounting suggests, and that China-based hackers have acquired data on a large number of major weapons systems and many minor ones. One former intelligence official described internal Pentagon discussions over whether another Lockheed Martin fighter jet, the F-22 Raptor, could safely be deployed in combat, because several subcontractors had been hacked.

In 2007-2008, the Pentagon gave secret briefings to about 30 defense companies alerting them to the aggressive spying effort and providing data to help defend against it, according to a person familiar with the process. The person did not know whether QinetiQ received the classified intelligence.

141 Attacks

Investigators eventually identified the Shanghai-based hackers that broke into QinetiQ as a crack team, nicknamed the Comment Crew by security experts, which has also hit major corporations and political figures, including the 2008 presidential campaigns of Barack Obama and John McCain. At least one other Chinese hacking team also may have been involved, according to a person familiar with the investigation.

In a Feb. 18 report, Mandiant, an Alexandria, Virginia- based security firm, attributed 141 major cyberattacks to the Comment Crew without naming the targets. Mandiant identified the Comment Crew as the People's Liberation Army Unit 61398, which is similar in some respects to the U.S. National Security Agency. Mandiant's report prompted Tom Donilon, President Obama's national security adviser, to call on China to stop the hacking of U.S. companies.

The spying on QinetiQ and other defense contractors appears aimed at helping China leapfrog the U.S.'s technologically- advanced military, foregoing years of research and development that would have cost billions of dollars, according to Michael Hayden, former director of the CIA.

China's military may also have stolen programming code and design details that it could use to disable some of the most sophisticated U.S. weaponry.

'Major Embarrassment'

The lengthy spying operation on QinetiQ jeopardized the company's sensitive technology involving drones, satellites, the U.S. Army's combat helicopter fleet, and military robotics, both already-deployed systems and those still in development, according to internal investigations. Jennifer Pickett, a spokesman for QinetiQ, declined to comment as part of a general policy not to discuss security measures.

"God forbid we get into a conflict with China but if we did we could face a major embarrassment, where we try out all these sophisticated weapons systems and they don't work," said Richard Clarke, former special adviser to President George W. Bush on cybersecurity.

The spies' trail at QinetiQ begins in late 2007, and so do the company's mistakes. QinetiQ's travails are documented in hundreds of unvarnished e-mails and dozens of reports that were never meant to be public, part of a cache that was leaked in 2011 by the group Anonymous after it hacked HBGary Inc., a Sacramento-based computer security firm hired by QinetiQ the previous year.

Team Outmaneuvered

The e-mails and reports are authentic, according to former HBGary executives and Day. Day agreed to an interview limited to the investigation's findings because the documents had already become public.

By reviewing the documents with security experts and interviewing more than a dozen people familiar with the QinetiQ breaches, Bloomberg News reconstructed how the hackers outmaneuvered QinetiQ's internal security team and at least five companies brought in to help salvage the situation.

Headquartered in a glass-and-steel office tower in McLean, Virginia, QinetiQ's U.S. subsidiary is a boutique arms maker, less than one-tenth the size of industry giants like Lockheed or Northrop Grumman Corp. (NOC) It has specialized in fields expected to grow as the rest of the Pentagon budget shrinks, including drones, robotics, software and high-speed computing. A 2012 want ad for QinetiQ's Albuquerque facility solicited a programmer to work on a "satellite-based global monitoring system" and limited candidates to those with top secret clearances only.

Stolen Data

In December 2007, an agent from the Naval Criminal Investigative Service contacted the company's small security team and notified them that two people working in McLean were losing confidential data from their laptop computers, according to an internal report. The agency had stumbled upon the stolen data as part of another investigation and the alert was a courtesy.

The San Diego-based agent didn't provide the identity of the hackers, who had been tracked by U.S. intelligence since at least 2002, or the crucial -- but classified -- fact that they were hitting other defense contractors. The company wouldn't find out who its attackers were for two more years.

QinetiQ put strict limits on the investigation.

"They just felt like it was this limited little thing, like they'd picked up some virus," said Brian Dykstra, a forensics expert based in Columbia, Maryland, which QinetiQ hired to conduct the investigation.

Four Days

Dykstra was given only four days to complete his work. He said the company didn't give him the time or data necessary to determine whether more employees had been successfully targeted, a standard precaution. In his final report, Dykstra warned that QinetiQ "is likely not seeing the full extent" of the intrusion.

Evidence surfaced almost immediately that he was right, as the attacks continued. On Jan. 7, 2008, NASA alerted the company that hackers had tried to infiltrate the space agency from one of QinetiQ's computers.

QinetiQ treated a series of attacks over the next several months as isolated incidents. The hackers followed a more meticulous strategy: In the first 2 1/2 years, they gathered more than 13,000 internal passwords and

raided servers that could give them detailed information about the company and how it was organized -- data they would use to devastating effect.

Security Holes

More investigations uncovered more security holes. In 2008, a security team found that QinetiQ's internal corporate network could be accessed from a Waltham, Massachusetts, parking lot using an unsecured Wi-Fi connection. The same investigation discovered that Russian hackers had been stealing secrets from QinetiQ for more than 2 1/2 years through a secretary's computer, which they had rigged to send the data directly to a server in the Russian Federation, according to an internal investigation.

QinetiQ's executives in the meantime fretted about rising costs.

"You could spend all your resources chasing such things as this," William Ribich, the former president of QinetiQ's Technology Solutions Group, said in an interview in January. Ribich, who retired in November 2009, shortly after the discovery of a major data theft, said he needed to balance the uncertain risk that the hackers could use what they stole against a growing shopping list of security products and consulting fees.

'Move On'

"You finally have to reach a point where you say 'let's move on,'" he said.

China's hackers in fact zeroed in first on Ribich's division, based in Waltham, and specifically on QinetiQ's drone and robotics technology. Internal reports leaked by Anonymous chronicle a breach at TSG in February 2008, followed by another attempt in March of that year. By 2009, the hackers had almost complete control over TSG's computers, the documents show.

Over one stretch in 2009, the spies spent 251 days raiding at least 151 machines, including laptops and servers, cataloging TSG's source code and engineering data. The hackers dribbled data out of the network in small packets to avoid detection, managing to get away with 20 gigabytes before they were finally stopped, according to an internal damage assessment.

The stolen cache included highly sensitive military technology and was equivalent in size to 1.3 million pages of documents or more than 3.3 million pages of Microsoft Excel spreadsheets.

Secrets 'Gone'

"All their code and trade secrets are gone," Phil Wallisch, senior security engineer at HBGary, wrote in an e-mail after being briefed on the loss by the company.

It was about to get much worse.

While QinetiQ's team tripped from crisis to crisis, the hackers honed their skills. They were next spotted in March 2010, after signing on with the stolen password of a network administrator based in Albuquerque, New Mexico, Darren Back.

The hackers logged on through the company's remote access system, just like any employee. It was a trick they were able to use only because QinetiQ didn't employ two-factor authentication, a simple device that generates a unique code employees enter, along with their usual password, anytime they work from home.

The problem had been spotted months earlier in a security review. Mandiant, which worked on several TSG breaches and performed the test, recommended a relatively inexpensive fix. The advice was ignored, according to a person familiar with the report.

Digital Secrets

In four days of furious activity, the hackers rifled at least 14 servers, taking particular interest in the company's Pittsburgh location, which specialized in advanced robotics design. The Comment Group also used Back's password to raid the computer of QinetiQ's Huntsville, Alabama-based technology control officer, which contained an inventory of highly sensitive weapons-systems technology and source code throughout the company. The spies had got their hands on a map to all of QinetiQ's digital secrets.

They also had begun to broaden their attack. As evidence mounted that the hackers had moved to divisions beyond TSG, QinetiQ hired two outside firms in April 2010 -- Terremark (TMRK) and a relatively new start up called HBGary, headed by Greg Hoglund, a former hacker turned security expert.

Glitches Surfaced

HBGary installed specialized software on more than 1,900 computers, then scanned the machines for snippets of malicious code. Glitches surfaced almost immediately. The software wouldn't load on at least a third of the computers, and even where it did, it missed some that the hackers' spyware was known to have infected, according to internal HBGary e-mails.

Matthew Anglin, an information-security principal at QinetiQ, whose job was to coordinate the two investigations, fretted that he had no idea what was happening in his own network. He complained that the expensive outside experts didn't seem to have a handle on what was going on, and wasted time tracing innocuous if unauthorized software.

The consultants also squabbled. HBGary complained in one report that Terremark was withholding vital information. Terremark countered that it appeared the hackers knew HBGary was hunting them and were using its technology to delete evidence of their presence on machines.

"They think we tipped off the attackers," Wallisch, HBGary's principal investigator on the project, wrote in an e- mail.

Every Corner

The security teams found evidence that the hackers had burrowed into almost every corner of QinetiQ's U.S. operations, including production facilities and engineering labs in St. Louis, Pittsburgh, Long Beach, Mississippi, Huntsville, Alabama and Albuquerque, New Mexico, where QinetiQ engineers work on satellite-based espionage, among other projects.

By the middle of June 2010, after weeks of intense work, the investigators believed they had cleaned QinetiQ's networks and began wrapping up.

The calm lasted a little more than two months. In early September, the FBI called QinetiQ with evidence that the defense contractor was again losing data, according to e-mails and a person involved in the probe. Anglin messaged both HBGary and Terremark, asking how quickly their teams could return.

Within hours of their arrival, the investigators again began finding malicious software, or malware, in computers throughout the company's North American divisions. Some of it had been there since 2009.

Software Deleted

It began to dawn on the security teams that the hackers had established a near permanent presence in the defense contractor's computers, mining new information almost as soon as it was written onto hard drives. "Oh yeah...they are f'd," Wallisch wrote to Hoglund in September.

Investigators also had to contend with frustrated QinetiQ employees. Upset about how much computer power the HBGary detection software was consuming, workers began deleting it from their computers with the approval of the company's information technology staff.

As the hunt continued, more clues surfaced about what secrets the spies were after. The hunters' digital footprints were found on the computers of QinetiQ's chief operating officer, a division vice president and dozens of engineers and software architects, including several with classified clearances.

Military Robots

Among the victims was a specialist in the embedded software on microchips that control the company's military robots, which would help in China's own robot-building program, said Noel Sharkey, a drones and robotics expert at Britain's Sheffield University. The PLA unveiled a bomb disposal robot in April 2012 similar to QinetiQ's Dragon Runner.

The chip architecture could also help China test ways to take over or defeat U.S. robots or aerial drones, Sharkey said.

"You could set them up in a simulation board and hack into them," he said. "That's standard stuff."

The spies also took an interest in engineers working on an innovative maintenance program for the Army's combat helicopter fleet. They targeted at least 17 people working on what's known as Condition Based Maintenance, which uses on-board sensors to collect data on Apache and Blackhawk helicopters deployed around the world, according to experts familiar with the program.

The CBM databases contain highly sensitive information including the aircrafts' individual PIN numbers, and could have provided the hackers with a view of the deployment, performance, flight hours, durability and other critical information of every U.S. combat helicopter from Alaska to Afghanistan, according to Abdel Bayoumi, who heads the Condition Based Maintenance Center at the University of South Carolina.

Redstone Arsenal

The hackers also may have used QinetiQ to break into the Army's Redstone Arsenal through a network shared with QinetiQ's engineers in nearby Huntsville. A breach of the base, home of the Army's Aviation and Missile Command, was linked by military investigators back to QinetiQ, according to a person familiar with the investigation.

It wasn't the only time the hackers used the same back-door approach to federal computers. The same person said that as recently as last year, federal agents were looking into a breach at a QinetiQ cybersecurity unit, which they suspected Chinese hackers were using in attacks against government targets.

The security lapses at QinetiQ led to investigations by several federal agencies, including the FBI, Pentagon, and Naval Criminal Investigative Service, according to two people involved, who didn't know the final outcome of the probes.

State Department

The State Department, which has the power to revoke QinetiQ's charter to handle restricted military technology if it finds negligence, has yet to take any action against the company. Two former federal law enforcement officials said that, despite its authority, the State Department lacks the computer forensics expertise to evaluate the losses and neither could recall department involvement in several major data theft investigations.

"In this case it looks like years go by without seeing any learning curve and that's what's scary," said Steven Aftergood, who directs the Project on Government Secrecy at the Federation of American Scientists. "The company is responsible for its own failures, but the government is responsible for the inadequacy of its response."

QinetiQ's U.S. operations are overseen by a proxy board that includes Riley Mixson, the Navy's former air-warfare chief. The board was briefed several times about the hacking and the investigations. In a brief telephone interview, Mixson said that "everything was duly reported" and then hung up the phone. Tenet declined to comment.

Probe Impact

The investigations didn't affect the company's ability to win government contracts, even to provide cyber-security services to federal agencies.

In May 2012, QinetiQ received a $4.7 million cybersecurity contract from the U.S. Transportation Department, which includes protection of the country's critical transport infrastructure.

"When it comes to cyber security QinetiQ couldn't grab their ass with both hands, so it cracks me up that they won," Bob Slapnik, vice president at HBGary, wrote after QinetiQ received a grant from the Pentagon in 2010 to advise it on ways to counter cyberespionage.

In the fall of 2010, Terremark sent a report to Anglin concluding that QinetiQ had been targeted by the Comment Crew since 2007 and that the hackers had been operating continuously in their networks since at least 2009. The report was part of the trove of documents leaked by Anonymous.

Complete Control

In that time, the hackers had gained almost complete control over the company's network. They had operated unhindered for months-long stretches and they had implanted multiple, hidden communications channels to extract data. Privately, the investigators concluded that the spies had gotten everything they wanted from QinetiQ's computers.

"My feeling is that if an attacker has been in your environment for years, your data is gone," Wallisch wrote in an e-mail to a colleague in December 2010, a few weeks before HBGary itself was hacked and the record stops.

"Everything about your business is known, cataloged, analyzed, by your enemy," Wallisch wrote. "I don't feel a sense of urgency anymore."

Table of Contents

Getting Inside the Head of Italian PSYOPS: Interview with Colonel Marco Stoccuto

By Richard de Silva, Defence IQ, 05/02/2013

Colonel Marco Stoccuto is an Information Operations and PSYOPS subject matter expert at the Italian Centre of Excellence for Joint Targeting Influence and former commander of the Italian 28thPSYOPS regiment. In recent years, he has deployed as Chief KLE at ISAF HQ and as Chief of IO at the NRDC-Italy. He spoke with Defence IQ ahead of his participation in Information Operations Global 2013. Below is a transcript of the interview but please click here to listen to the full audio version.

Colonel, to what extent is Information Operations and PSYOPS a priority for Italian forces and how is it integrated with modern operations?

Italian Armed Forces have experimented with an interesting amount of experiences across different Theatre-of-Operations and collected lessons from all of these environments, characterized by a wider presence of means of communications in asymmetric scenarios.

The awareness of the critical role carried out by psychological operations within the overall Info Ops campaign as instruments to attract local consensus and enhance force protection, is taking over more and more in the Italian approach to conducting operations.

The level of priority is underlined by the high level of attention toward the development of all those units liable of supporting the interaction within the Information Environment (with respect both to the human perspective of the decisional process and the automation systems responsible for the transmission, collection and process of information) as well as the development of a coherent doctrinal body integrating traditional methodologies alongside those operating directly in the area of perception, in order to influence the target audiences.

The clear understanding of their critical role in all different type of operations – moreover of its crucial part in the peace keeping ones – is systemically modifying our way of drafting the operations, merging the kinetic and the non-kinetic dimensions.

We are affirming a doctrinal determination to make use of such capabilities to positively present the campaign and concurrently to mitigate the undesired consequences of military actions whose effects might hamper the relationship with locals and induce an increase in the overall menace to the achievement of the Force's objectives.

The Italian Army is therefore empowering capabilities by allocating a high priority to them, aiming at achieving a role of excellence both at joint and international level.

Benchmarking or measuring results and value is notoriously difficult in this domain. In what ways can strategic communicators potentially evaluate their methodology?

In the non-military world, mainly the commercial one, in which marketing rules apply, it is definitively easier to benchmark results. In our domain, however, to weigh the level of persuasion is difficult and often empirical.

In my experience, I have often seen a large gap between different assessments of effectiveness in our communication efforts. Most of the time the subjectivity of the assessment, overtaking any methodology, represented the extent of the measurement… and most of the time, it failed.

Although many think tanks assert that the effect methodology is no longer valuable, I still sense it is on the right path. Every time we undertake a communication campaign at strategic level as well as a communication effort at tactical level, we expect to persuade our target audience to change behaviours; that means to act or not to act.

There are two critical aspects in our Strategic Communication Campaign to enable the measurement: one is the correct identification of those expected actions, reactions and non-actions representing the indicators of a modifying behaviour and attitude at different levels; and the second is represented by the correct identification of the threshold signifying the pursuit of those effects, whose synergy is liable to establish the achievement of an objective.

From my viewpoint, the most sensitive effort resides in the analytical identification of those indicators enabling the assessment of changes. They are to be very consistent with the local cultural perspectives and cleared from our point of view.

The communication campaign's focus always has to view the CoG of the Population as a pyramid that is effected from the tactical to the strategic level and must be mutually supportive. Communication in its wider understanding is addressed to an ample audience with the ability to induce modifications.

The Arab Spring is a clear example. The effects in terms of communication are evident but the result are affected by a still foggy perception of the most effective communicator.

What recent approaches and successes could you highlight in the contemporary information operations field, such as in Afghanistan? To what extent can these tactics apply to other campaigns, or is there too much of a variation in culture or adversary to appropriately rework the same tactics?

Honestly, the effort to claim that contemporary Information Operations have been a success in Afghanistan, as well as Iraq, might be daring, although the eleven years of the campaign have actually induced and shaped the conduct of such a operational functions to the level of science. If we compare the traditional C2W best practice applied in Kosovo – and even before in BiH – the current concept of Information Operations is actually a science. However, my personal perspective identifies the current development as peculiar to the Afghan Theatre of Operations and shaped around its own specific culture.

We have learned quite a lot about recognising peculiarities and understanding different cultures, in order to enter in the mind of our TA. However we still have a gap in applying the correct approach to achieve the heart or even better his stomach. When I started joining this community 8 years ago no one was used to talk about KLE or engagement at all. Now we understand how critical is to talk appropriately to the people, to the right people and how dangerous is mismatching words and deeds.

Iraq proved to be a struggle for power for the central government and despite the claim of willingness to reach the heart of common people, the settlement occurred only once the parties achieved a balance in power.

Afghanistan is more patch-work and crosses over safe havens for terrorism, religious fundamentalism and illicit economical pursuits.

So no, I don't think that the Afghan model can be exported "sic et simpliciter" as it is in a different cultural situation. We can instead make use of a few best practices, of which the most relevant in my opinion are the procedural approach liaising all the tool of communication both internal and external; the process of planning and carrying out all those activities aimed at pursuing the influential objectives; and above all, the deepest and most highest-reaching possible engagement at all levels in order for us to sing from the same hymn sheet, preventing gaps and weakness exploitable by the adversary propaganda.

That said, most of the future campaigns will be dictated by a comprehensive and overarching understanding of the Information Environment both in its cognitive and informational domain, providing an early premise to the development of the campaign itself and to the identification of a competitive Narrative, tying up all the relevant aspects likely to reach "the belly before the mind" of our TAs.

What do you hope to learn about at Information Operations Global 2013, particularly from our non-military attendees/speakers?

The comprehensive approach is more and more interlinking the military world and the non-military one.

Long time before we started talking about Information Operations, in the profit environment of marketing the requirement for influencing customers started becoming an issue.

However the military world has undertaken a great effort to raise such a concept to the dignity of operational function after understanding the need to affect will before capabilities.

Finally such an improvement of techniques has spilled out of the peculiar military environment as operational functions, becoming an appealing area of study for those companies and organizations seeking to address and influence people in a worldwide more and more competitive market.

Beyond the final scope, the common aims resides into influencing and persuading different target audience groups to change attitude and behaviours, and I do believe that an exchange of perspective between military and non military world is surely beneficial.

It might be revealing and surfacing commonalities and good advices in order to optimize our techniques as well. Very often we, as military, are inclined to discharge those developments occurred in the non-military realm, claiming that the original purposes have been diverted.

We underestimate the importance of profit as actual engine for the researches of those enterprises, which scope is to sell a product and cannot afford missing the target twice. They as well are making every effort to understand the social and cultural norms which colour the environment.

The Influencing is so much overlapping the marketing concept, that the mutual knowledge between military and non-military is paramount and I deem beneficial for both, enabling a better understanding of the mechanics of human behaviour and the related dynamics that administrate the persuasion.

Table of Contents

Understanding Groupthink

By Keith Vore, Small Wars Journal, 8 April 2013

Madness is the exception in individuals, but the rule in groups. — Friedrich Nietzsche

The brigade staff had assembled to discuss the upcoming mission with its commander. Time was short, and pressure intense. "This is the last thing we need right now, given everything else on our plate," muttered the brigade XO under his breath. The commander quickly discussed the essence of his mission analysis, gave curt guidance on a course of action he deemed suitable to accomplish the mission, and left the room. The brigade XO and S3—both of whom had strong, dominant personalities—discussed between themselves a way ahead, and then began barking orders to the rest of the staff in order to get the mission planned as soon as possible.

A couple of the brigade staff's deep thinkers, junior in grade to the rest, began thinking of all kinds of challenges with the commander's guidance for the upcoming mission. They each approached the brigade XO separately, only to be sternly rebuked for stepping out of line. "Get on the team, pal—the boss told us what he wants. Team play is our mantra here." Needless to say, the reaction on the part of the other staff members was to quickly sidle up to "the plan" as it unfolded, without challenging any aspect of it. The longer everyone participated in the planning process, the more everyone seemed to get comfortable with its concept. That is, they became increasingly complaisant.

The brigade commander and staff had stereotyped its adversary, underestimating his sophistication. Too many unchallenged assumptions led to too many surprises. In a couple of instances, externally-provided information that would have opened everyone's eyes during planning had been shooed away by either the brigade XO or S3. Finally, new information which came to light late in the planning process—and which would have completely revealed the flaws of the plan's concept—was summarily dismissed by the staff: "This is obviously a case of erroneous information." While the staff assembled the plan in record time, the mission failed.

Sound familiar?

Is Groupthink Commonly Understood? In a recent Infinity Journal article, retired U.S. Marine Corps Lieutenant General Paul Van Riper credits Scottish military historian Hew Strachan with contending that the word 'strategy' has acquired "a universality which has robbed it of its meaning, and left it with only banalities."[1] Strategy is an example of a term we use so often that we risk desensitizing its meaning, or perhaps settle upon a more simplified definition. In communicating ideas, it is questionable whether simplified terms with complex meaning like this convey the same things to everyone.

We contend that the term "groupthink" falls into this category. Groupthink is a term used within the U.S. military, as well as the broader civilian business world. Asking what groupthink consists of, however, often elicits an upward roll of the eyes. "Everyone knows what groupthink is," goes the unspoken response, implying the self-evident nature of the term. The truth of that opinion is debatable.

The purpose of this article is to enhance understanding of groupthink, by reintroducing the psychologist who coined the term. We will also establish groupthink-related causes, and groupthink mitigation techniques. The article then concludes by pondering who might be best suited to guard against groupthink's onset.

To illustrate the nuanced challenges of groupthink, we informally surveyed a small group of Intermediate Level students at one of the Defense Department's educational institutions. The students were junior field grade officers from joint and international services, nearing the end of their year-long education. Our survey asked two questions: 1) Whether their education had formally addressed groupthink as a subject; and 2) What were groupthink's causes? A little more than half of the group responded that while groupthink had been discussed early in their education year, albeit briefly as part of a broader class topic, groupthink was not a central focus of the class. In response to the causes of groupthink, about half of the group cited dominant personalities within a group who ignored dissenting opinions, and the inclination of group members to remain within the group's good graces by avoiding dissention. Less than one-fourth of the responses cited direct pressure on any member who objected to group opinions.[2] What strikes us is not what the students said, but what they did not say. Their responses, when compared to the written material on groupthink, reflect a basic but limited understanding of the topic, and suggest room for improvement.[3]

What is groupthink, beyond the ideas that some of the students surfaced above? How do we deal successfully with groupthink, if we don't fully understand what it is? How do we spot groupthink's causes when they arise, and take measures to mitigate them? Dr. Irving Janis provides answers.

Irving Janis and Groupthink. Irving Janis studied accounts of the Kennedy Administration's deliberations during the Bay of Pigs crisis, which occurred less than three months after President Kennedy's inauguration. Based upon a plan inherited from the Eisenhower administration, Kennedy and his national security advisors debated internally whether to proceed. The resulting decision to support the invasion of Cuba was a fiasco.

"How could we have been so stupid?" demanded John F. Kennedy after his administration's invasion of Cuba had been soundly defeated at the Bay of Pigs. The invasion was one of the most ill-conceived in American history. Yet the planners of this operation included some of the smartest people in America. They didn't fail because they were stupid. They failed because Kennedy and his advisors stumbled over the most common traps lurking in group decision-making terrain. They agreed prematurely on the wrong solution. Inadvertently, they gave each other biased feedback that made the group as a whole feel certain that it was making the right choice. They discouraged each other from looking at the flaws in their assumptions. And they ignored dissenters who tried to speak up.[4]

Janis was curious why the intelligent men of the Kennedy administration could have made such a blunder. He wondered whether they had succumbed to a psychological condition associated with social conformity—whether these individuals were more interested in maintaining the approval of fellow group members than of stating their minds and challenging various notions within the group.[5]

Janis' study approach was to analyze the decision making faults and the group psychology of President Kennedy's Executive Committee (EXCOM) during the Bay of Pigs crisis. From this analysis, he synthesized a framework of groupthink causes, which he subsequently compared to other U.S. national security incidents—among them Pearl Harbor, the escalation of the Vietnam War, and the Cuban Missile Crisis. After analyzing these other incidents, Janis was able to solidify his groupthink framework. He published his results in a 1972 book, Victims of Groupthink; an updated version appeared in 1982, entitled Groupthink.

Janis observed several faults in decision making, which he believed contribute to groupthink. Said differently, these kinds of decision making errors prepared the ground for groupthink to occur. These faults are the following:

* Group discussion limited to a few alternative courses of action.
* Inadequate group survey of objectives to solve the problem.
* Failure of the group to reexamine a course of action preferred by the group after new evidence revealed risks to that course of action.
* Group neglect of courses of action originally rejected, in spite of new information that ameliorates that risk.
* Group disinclination to seek external opinion.
* Selective bias in processing information provided by external sources.
* Group neglect in devoting adequate time to consider how the chosen option might fail.

Additionally, Janis felt that any given group might also succumb to other "common causes of stupidity…erroneous intelligence, information overload, fatigue, blinding prejudice, and ignorance."[6]

Janis asserted that an informal correlation exists between the decision making faults (above) and what he synthesized as eight causes of groupthink. These eight causes, paraphrased, are as follows:

* A group illusion of invulnerability (vis-à-vis the object of planning), leading to excessive optimism and risk taking; this cause presumes an inherent intellectual or physical superiority.
* Unquestioned belief in the group's inherent morality (vis-à-vis the object of planning).
* Group efforts to dismiss information that might require reconsideration of assumptions.
* Stereotyped views of enemy leaders.
* An inclination toward "self-censorship": this is a reaction on the part of individuals, who suppress personal doubt and counterargument in the interest of the larger group.
* An illusion of unanimity: this occurs where members implicitly presume the entire group holds a particular set of views, when in fact those views differ widely, and are unstated.
* Direct pressure on members who do expresses contrary arguments, since those contrary arguments disrupt team unity.
* Self-appointed "mind guards"—members who protect the group from hearing contrary information.[7]

Based on his analysis, Janis goes on to define groupthink:

> I use the term 'groupthink' as a quick and easy way to refer to a mode of thinking that people engage in when they are deeply involved in a cohesive in-group, when the members' strivings for unanimity override their motivation to realistically appraise alternative courses of action... Groupthink refers to a deterioration of mental efficiency, reality testing, and moral judgment that results from in-group pressures.[8]

Admittedly, Dr. Janis' research focused at the level of US national security. One could argue that some of his observations, as verbalized, have limited merit within tactical military echelons. We disagree. For example, whereas Janis stipulates that a group's illusion of invulnerability—or an unquestioned belief in the group's inherent morality—are groupthink causes, certainly battalion- through corps-level staffs could succumb to these same kinds of causes during operations within the counterinsurgency realm, or while operating within foreign environments. Rather, we believe that Janis' groupthink causes transcend a particular type or echelon of unit.

Earlier in this article, we mentioned that we informally surveyed Intermediate Level students about groupthink. Half of them cited causes of either 1) dominant personalities within a group who ignored dissenting opinions, or 2) the inclination of group members to remain within the group's good graces by avoiding dissention. Less than one-fourth of the surveyed students cited direct pressure on any member who objected to group opinions. Based upon the ideas discussed thus far, what didn't those students say? Which of Janis' groupthink causes lay outside of those student responses? The students' rather simplistic responses missed several causes that Janis cited: any reference to a group's illusion of invulnerability toward the object of planning—a presumption of superiority; allowing the group to express optimism and take excessive risk; the unquestioned belief in the inherent morality of the group; and stereotyping of enemy leaders. All of these could be related to an implicit U.S. cultural mindset, hidden from view. They did not identify a group's "illusion of unanimity" that Janis cites as a groupthink cause, nor was there any mention of "self-appointed mind guards." Finally, Janis asserted that when a group commits any one of several decision making errors, then fertile ground exists for groupthink to occur. None of the surveyed students identified that correlation.

Overall, while the surveyed students hit some of the high points, their level of understanding was basic. If Janis' assertions are correct, and avoidance of groupthink is important, one should recognize the need for increased emphasis in the education of groupthink.

Groupthink Mitigation Techniques. To mitigate the effects of groupthink, Dr. Janis suggests several measures:

* The leader of groups should assign to each member the role of critical evaluator, and solicit objection and doubt. The leader, in turn, should be open to group objections and doubts.
* The group leader should refrain from providing personal opinions to the group at the outset, so as to preclude group members from inferring "what the boss wants."
* The group should establish several independent sub-groups to examine the same objective, to determine multiple ideas for the same issue.
* During its deliberations, the group should actively solicit external feedback on its positions, and be careful not to rationalize away feedback inconsistent with its views.
* The group should also invite into its deliberations external expertise to challenge the group's views.
* One or more of the group's members should be specifically assigned the role of devil's advocate to challenge the group's views. This role should be rotated among the group's members during deliberations.
* After the group reaches consensus on its planning objective, it should convene a final meeting at which any remaining doubts or challenges might be offered.[9]

In their decision making book Winning Decisions, authors J. Edward Russo and Paul Schoemaker offer additional suggestions to mitigate groupthink:

* The group's members should not take sides too soon in decision making deliberations; better to defer judgment and hear all of the discussion first.
* The group must have established norms which support conflict (in debate); this supports the idea that "task conflict" is an important element of decision making, while remaining on the lookout for (and avoiding) "relationship conflict." There are several ways to establish "conflict norms":
* Ensure the group is heterogeneous. Diversity among group members enhances the opportunities for insight and alternative perspective. Individuals with wide variance in backgrounds, as well as difference in age, help establish heterogeneity.
* Require group members to "precommit": to establish, in writing before deliberation begins, what each member believes the best ideas in solving the problem might be. This practice, ideally, prevents each member from becoming tainted by others' opinions once debate begins.
* Solicit more than one option from each member individually. Don't allow members to sit back and relax, relying upon the option-generating prowess of fellow group members.
* Solicit and use reports from minority members of the group to ensure that potentially useful alternative perspectives are not drowned out by the majority.[10]

Who Is Inclined To Identify Groupthink and Suggest Mitigation Techniques? Who, on each military staff, is inclined to identify the causes of groupthink as they emerge? Who has the knowledge of mitigation techniques to recommend their adoption?

All of us…or at least all of us should. If individual staff members truly understand what groupthink is, what its causes are, and what kind(s) of mitigation techniques would work given a particular context, then theoretically

each member of a staff ought to be able to help prevent groupthink from occurring. While it sounds simple enough, however, even those who understand the details of groupthink might still feel powerless to face it directly.

Additionally, each staff element has a lens through which it views every problem, and its own set of focal points, time pressures and attendant products to provide. In a perfect world, the Chief of Staff/Executive Officer has the authority and responsibility to manage the entire group process. Accordingly, he/she ought to be able to act as the "groupthink monitor." Yet experience shows that this position seems to be most encumbered of all, and least able to devote enough time to the task while managing to accomplish everything else expected.

Decision support red teams have been documented for various Army units from brigade through Army Service Component Command, as well as in Unified Commands. The Marine Corps is also implementing red teams within its structure. Red teams exist to provide commanders an independent capability to fully explore alternatives in plans, operations, concepts, organizations and capabilities in the context of the operational environment and from the perspectives of partners, adversaries and others. Red teams typically report to the Chief of Staff/Executive Officer, and have staff-wide authorities to observe, challenge views, and provide alternative perspectives. Divorced from a specific staff element's narrower focus, as well as the time pressures to produce various products, the red team has the independence to think broadly about the task in a manner that ideally the Chief of Staff/Executive Officer should.

The red team, then, can take on the task of looking for causes of groupthink as they occur, or of recommending mitigation techniques should the need arise. The University of Foreign Military and Cultural Studies educates red team members in various courses at Fort Leavenworth. Its curriculum is devoted to self-awareness, critical thinking, and understanding culture from the perspective of cultural anthropologists. The curriculum includes (in addition to groupthink) topics such as cognitive biases, the role of theory, and applying a set of frameworks with which to analyze problems, including how to properly assume the role of devil's advocate.

Groupthink is a subject that has more to it than meets the eye, in spite of its self-evident name. Deeper understanding of groupthink, its causes, and mitigation techniques should help a commander and his staff prevent it from occurring, and red teams can assist in the cause. Forewarned is forearmed.

Notes:

[1] Paul Van Riper, "The Foundation of Strategic Thinking," Infinity Journal 2, no. 3 (Summer 2012), citing Hew Strachan, "The Lost Meaning of Strategy" in Survival (Autumn 2005), p. 34.

[2] The sample size of this group was 21 students, all of whom were enrolled in an elective on red teaming.

[3] This is not intended to cast aspersions upon the professional educators in the Defense Department's Intermediate Level and Senior Service academic institutions. All contend with a plethora of required topics, both joint- and service-related, and do so with finite limits on available time. Instead, it is an indication that the level of understanding about groupthink begs emphasis, especially for Intermediate Level students who will graduate and become general staff officers, as well as senior leaders of brigade and battalion staffs. All of them, in this capacity, will be subjected to staff work in intense environments and time pressures. Lacking depth of understanding, they will be prone to succumb to groupthink's magic.

[4] J. Edward Russo and Paul J.H. Schoemaker, Winning Decisions: Getting It Right The First Time (New York: Random House, 2002), p. 159.

[5] Irving L. Janis, Groupthink: Psychological Studies of Policy Decisions and Fiascoes (Boston: Wadsworth, 1982), p. vii.

[6] Ibid, p. 10.

[7] Ibid, pp. 174-175.

[8] Ibid, p. 9.

[9] Ibid, pp. 262-270.

[10] Russo and Schoemaker, pp. 169-175.

Table of Contents

Are Military Hackers Targeting Tibetan Activists?

By Christopher Watt, MaisonNueve, April 25, 2013

Lhadon Tethong was the first to open the email. How could anyone ignore the subject line? "Fwd: please save my Tibetan wife," it read. The email was sent on April 28, 2010. It was well written, "or at least it was better written than a lot of the messages we get that are full of spelling and grammatical mistakes," Tethong says. But it still seemed malicious. The name in the Yahoo email address was Nate Herman, but someone named Martin Lee signed off on the request for help. The text invited the recipient to click on a .zip file, apropos of nothing.

In May 2011, Tethong forwarded the email to the Citizen Lab, a University of Toronto research group that works with civil-society groups to fight cyber-attacks. The Citizen Lab is known for exposing a cyber-espionage ring called Ghostnet, which by 2009 had compromised nearly 1,300 computers in over one hundred countries, including some at the Dalai Lama's office in India. Tethong was working for Students for a Free

Tibet at the time, and, she says, its Gmail accounts regularly show login attempts from China and Hong Kong. Since China very much opposes a free Tibet, Tethong suspected the Chinese were behind the email.

Others increasingly suspect the Chinese, too. Chinese cyber-espionage already costs American businesses an estimated $100 billion in intellectual property losses a year, according to a recent National Intelligence Estimate. National Security Agency and US Cyber Command chief Keith Alexander has called this the greatest transfer of wealth in history. On February 19, a US security firm called Mandiant published one of the most detailed accounts of Chinese cyber-espionage ever. The report is called APT1: Exposing One of China's Cyber Espionage Units.

The Virginia-based Mandiant virtually nailed its findings to the front door of a twelve-storey building in Shanghai. Although it resembles an average apartment, the building is believed to be to headquarters of the People's Liberation Army (PLA) Unit 61398. Mandiant blamed the PLA for stealing intellectual property from 141 defense, aerospace, IT and law firms, plus a few think tanks, going back almost a decade. But Mandiant said little about non-governmental organizations like Students for a Free Tibet. Among the organizations included in the study, only six are civil-society groups, says Dan McWhorter, managing director of threat intelligence for the company. Mandiant stuck to companies that might have access to information about military technology.

But Mandiant did provide more data for follow-up research than most cyber security firms do, says Seth Hardy, a senior security analyst at the Citizen Lab. So Hardy decided to do some digging. He wrote up his findings in a February 25 post for Citizen Lab called "APT1's GLASSES—Watching a Human Rights Organization." It revisits the Students for a Free Tibet incident from 2010, and attributes the attack to the same group that Mandiant calls Unit 61398—although Hardy stops short of calling out the Chinese government by name.

Unit 61398 is also known as the Comment Crew because of signature remarks left embedded in code on compromised websites. Mandiant renamed it APT1, for Advanced Persistent Threat. If Mandiant is right, hundreds if not thousands of APT1 cyber-spies are waging espionage from within the Shanghai building. Explicitly attributing the crimes of individual actors to nation-states is controversial in cyber-circles, since network traffic can easily be disguised. But, argues McWhorter, either the PLA is the source of the attacks, or a freelance crew is using the Chinese army's neighborhood as its base and, somehow, in an authoritarian state, the government is not involved.

Mandiant has benefited from a new kind of Cold War alarmism about Chinese cyber-espionage, and the company's accusations have provoked denials from the Chinese government. Former Foreign Minister Yang Jiechi, the highest-level official to comment publicly so far, told reporters at a party conference, "Those reports may have caught the eye of many people, but they are built on shaky ground." Yang argued that China's critics want to "turn cyberspace into another battlefield, or capitalize on virtual reality to interfere in another country's internal affairs."

It probably didn't hurt Mandiant's business that, in the weeks before publication, the New York Times, among other news organizations, went public about its own dealings with suspected Chinese hackers. Those attacks, which Mandiant helped investigate, and attributed to a group it calls APT12, followed reports by the newspaper about corruption and family wealth at the highest level of Chinese politics.

But the stakes, and the tools available for preventing and responding to attacks, are different for civil-society groups like SFT, which can't afford to hire the likes of Mandiant—McWhorter acknowledges that its client base is "high-end"—and therefore turn to places like the Citizen Lab for help.

But who would target a small NGO? Adam Segal, an expert on China and cyber security with the Council on Foreign Relations, wrote following the alleged Chinese hack on the New York Times that data from non-corporate organizations is harder to monetize than blueprints and business plans, and thus there's less incentive for criminal hackers to attack; sometimes, a nation-state lurks in the background, prodding hackers against dissidents and gadflies who have run afoul of the authorities.

While Hardy's Citizen Lab report shows that APT1 is interested in specific political targets, not just corporations, others are not totally convinced by Mandiant's claim that APT1 has a regular mission from the Chinese government. Take Jeffrey Carr, author of Inside Cyber Warfare. Carr believes the Mandiant report suffers from analytical flaws, and he argues that Mandiant fails to eliminate other possibilities. Maybe the PLA and the hackers have an agreement, but that doesn't mean that APT1 is on the Unit 61398 payroll. Instead, the hackers might simply be trying to curry favour with the Chinese government. "While attacks against NGOs can reasonably ensure that a nation-state would be among the suspects, it doesn't eliminate non-state actors that may be seeking the favor of a nation state, or providing a favor in exchange for other paying work," Carr wrote in an email.

Chinese animus against Tibetan causes is well understood, and Chinese hackers, whether rogue or military-directed, have plenty of incentive to target Tibetan activists. More than a hundred Tibetans have set themselves on fire in recent months, ostensibly for a Tibet free from Chinese rule. For China, Tibet is an important piece of real estate that it currently runs as an "autonomous" province. "Without Tibet, mainland China would be much more susceptible to attack from India," says Jennifer Richmond, China director at Stratfor, a geopolitical intelligence firm. "The Tibetan plateau creates a defensible border that is imperative to the protection of the mainland and, barring a massive country-wide revolution, there is absolutely no policy in consideration that would allow Tibetan independence." Indeed, Carr wrote, it's "important to remember that there are thousands of Chinese hackers who don't like Tibet and they have a 20-year history of going after organizations who they believe have acted in an offensive manner against China."

James Lewis, a senior fellow at the Center for Strategic and International Studies, recently published an annotated bibliography of attacks attributed to China, going back to 2001. It mentions Ghostnet, the 2009 attacks on the Dalai Lama and others, which trace back to an intelligence facility operated by the Third Technical Department of the PLA on China's Hainan Island, in the South China Sea.

AlienVault Labs also tracks hackers in China. "There are several dozens of groups operating from China right now. Some of them focus on NGOs and activists and others are targeting a wide range of industries including activists," wrote director Jaime Blasco in an email. "My question is, guess who is the only one interested in targeting high profile entities in the US and Tibet/Uyghur activists around the world?"

But Seth Hardy says he hasn't seen enough evidence to directly attribute GLASSES, the targeted attack on SFT analyzed by the Citizen Lab, to the Chinese government. Same goes for the newer GOGGLES, described in the Mandiant report, which used the same compromised eyewear website to launch its attacks. In other words, Hardy understands what APT1 is doing, but won't say whom he thinks signs the checks.

Hardy might be more willing to blame the Chinese government if he had better information. "The problem with attribution is just because the data gets sent to a Chinese IP does not mean the attacker is even Chinese," he says. "There are any number of ways to redirect traffic." Hardy adds that, with "political issues, we don't make any statements of attribution unless we are absolutely sure."

It seems clear enough that someone wants to know American business secrets and spy on Tibetan activists. But forget, for now, trying to identify the primordial loyalties of the human behind the malware. Forget that the security-clearance-lacking masses don't quite know what China does with the intelligence it gathers, perhaps because the media's getting hacked just like everyone else, and even chased off from the Shanghai site by uniformed guards. What Seth Hardy does know is that APT1 tried to hack a Tibetan organization in 2010. (Due to Citizen Lab policy, he did not mention Students for a Free Tibet's name in his report, or in conversation, though Tethong confirmed that SFT was the organization in question.) Call the antagonists Comment Crew or APT1. They target people. They leave trails, more or less. Yet you'd have to call them professionals.

Table of Contents

DOD Forming Information Operations Executive Steering Group

By Molly Bernhart Walker, FierceGovernmentIT, May 6, 2013

The Defense Department will form an information operations executive steering group to better streamline IO, or the mechanisms the department uses to integrate and implement information-related capabilities during military operations, says a May 2 DoD directive (.pdf).

"The IO ESG will serve as the primary coordination forum within DoD to inform, coordinate, and resolve IO issues among the DoD Components and, as appropriate, deconflict IO issues as they are represented in established DoD policy and programmatic decision forums," says the directive.

Not only does the directive order the immediate formation of the steering group, it also updates the definitions of information operations, and establishes policy and responsibilities for IO, updating those laid out in a DoD directive that dates back to 1999.

In a recent survey on Federal IT Reform, Senior government IT executives laid out their vision for the coming year, detailing challenges and identifying priorities. To read more about these timely results click here to download the summary today.

The directive lays out the specific IO responsibilities for the undersecretaries of defense for policy; intelligence; acquisition, technology and logistics; personnel and readiness; and comptroller. It also enumerates IO responsibilities for the director of cost assessment and program evaluation, DoD component

heads, secretaries of military departments, chairman of the joint chiefs of staff, combatant commanders, commander of strategic command, commander of special operations and directors of defense agencies.

The IO ESG will unite all of these responsibilities into a coordinated effort, offering a complete view of information operations, says the directive.

"The IO ESG's organization, membership, policies, and procedures will be established in a separate DoD Instruction," says the document.

This directive does, however, note that the undersecretary of defense for policy will be one of the co-chairs of the IO ESG, who "establishes and maintains the IO ESG." The chairman of the joint chiefs of staff will also co-chair the IO ESG and "establishes and maintains Joint Staff participation in the IO ESG."

Table of Contents

Pentagon: China Views Information Warfare as Key to Countering U.S. Pacific Forces

By Bob Brewin, NextGov, May 6, 2013

China views cyber warfare as the essential element to attack U.S. forces operating in the western Pacific, the Defense Department reported today in its annual analysis of that country's military capabilities.

The Pentagon, in its report "Military and Security Developments Involving the People's Republic of China," said the People's Liberation Army views space operations as "the commanding point for the information battlefield." The report said PLA documents emphasized the necessity of "destroying, damaging and interfering" with an enemy's reconnaissance and communications satellite systems.

If China goes to war, the report said, the country plans to control information, sometimes to seize the initiative and gain an advantage in the early phases of a campaign to achieve air and sea superiority.

"China is improving information and operational security to protect its own information structures, and is also developing electronic and information warfare capabilities, including denial and deception, to defeat those of its adversaries," the report said.

Chinese doctrine puts a priority on computer network defense in peacetime, the report said. It views offensive information operations as an unconventional weapon, "which must be established in the opening phase of the conflict and continue during all phases of war," with all potential adversaries. China sees the United States as particularly "information dependent," the report said.

The report notes that China also uses cyber warfare as an espionage tool: "In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military," the report said -- a statement reinforced by David Helvey, deputy assistant secretary of Defense for East Asia, at a Pentagon press briefing today.

Computer network intrusions detected in 2012 "were focused on exfiltrating information. China is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs," the report said.

China is acquiring a range of technologies to enhance its counter-space capabilities so in time of war it can "bind and deafen the enemy," according to PLA writings, the report said, while at the same time beefing up its own space systems.

In December 2012, China turned on a regional navigation system to rival GPS. It plans to launch 100 satellites through 2015. The launches include imaging, remote sensing, navigation, communication, and scientific satellites, as well as manned spacecraft, the report said.

While the report depicts an increasingly robust and high-tech Chinese military, the country's defense budget of $114 billion announced on March 13 amounts to just over 20 percent of the Pentagon's 2014 budget request of $526.6 billion.

Helvey said that Defense lacks total insight into the Chinese military budget. He estimated that it ranges between $135 billion and $215 billion.

Table of Contents

US Directly Blames China's Military for Cyberattacks

By David E. Sanger, New York Times, 7 May 2013

WASHINGTON — The Obama administration on Monday explicitly accused China's military of mounting attacks on American government computer systems and defense contractors, saying one motive could be to map "military capabilities that could be exploited during a crisis."

While some recent estimates have more than 90 percent of cyberespionage in the United States originating in China, the accusations relayed in the Pentagon's annual report to Congress on Chinese military capabilities were remarkable in their directness. Until now the administration avoided directly accusing both the Chinese government and the People's Liberation Army of using cyberweapons against the United States in a deliberate, government-developed strategy to steal intellectual property and gain strategic advantage.

"In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military," the nearly 100-page report said.

The report, released Monday, described China's primary goal as stealing industrial technology, but said many intrusions also seemed aimed at obtaining insights into American policy makers' thinking. It warned that the same information-gathering could easily be used for "building a picture of U.S. network defense networks, logistics, and related military capabilities that could be exploited during a crisis."

It was unclear why the administration chose the Pentagon report to make assertions that it has long declined to make at the White House. A White House official declined to say at what level the report was cleared. A senior defense official said "this was a thoroughly coordinated report," but did not elaborate.

Missing from the Pentagon report was any acknowledgment of the similar abilities being developed in the United States, where billions of dollars are spent each year on cyberdefense and constructing increasingly sophisticated cyberweapons. Recently the director of the National Security Agency, Gen. Keith Alexander, who is also commander of the military's fast-growing Cyber Command, told Congress that he was creating more than a dozen offensive cyberunits, designed to mount attacks, when necessary, at foreign computer networks.

When the United States mounted its cyberattacks on Iran's nuclear facilities early in President Obama's first term, Mr. Obama expressed concern to aides that China and other states might use the American operations to justify their own intrusions.

But the Pentagon report describes something far more sophisticated: A China that has now leapt into the first ranks of offensive cybertechnologies. It is investing in electronic warfare capabilities in an effort to blind American satellites and other space assets, and hopes to use electronic and traditional weapons systems to gradually push the United States military presence into the mid-Pacific nearly 2,000 miles from China's coast.

The report argues that China's first aircraft carrier, the Lianoning, commissioned last September, is the first of several carriers the country plans to deploy over the next 15 years. It said the carrier would not reach "operational effectiveness" for three or four years, but is already set to operate in the East and South China Seas, the site of China's territorial disputes with several neighbors, including Japan, Indonesia, the Philippines and Vietnam. The report notes a new carrier base under construction in Yuchi.

The report also detailed China's progress in developing its stealth aircraft, first tested in January 2011.

Three months ago the Obama administration would not officially confirm reports in The New York Times, based in large part on a detailed study by the computer security firm Mandiant, that identified P.L.A. Unit 61398 near Shanghai as the likely source of many of the biggest thefts of data from American companies and some government institutions.

Until Monday, the strongest critique of China came from Thomas E. Donilon, the president's national security adviser, who said in a speech at the Asia Society in March that American companies were increasingly concerned about "cyberintrusions emanating from China on an unprecedented scale," and that "the international community cannot tolerate such activity from any country." He stopped short of blaming the Chinese government for the espionage.

But government officials said the overall issue of cyberintrusions would move to the center of the United States-China relationship, and it was raised on recent trips to Beijing by Treasury Secretary Jacob J. Lew and the chairman of the Joint Chiefs of Staff, Gen. Martin E. Dempsey.

To bolster its case, the report argues that cyberweapons have become integral to Chinese military strategy. It cites two major public works of military doctrine, "Science of Strategy" and "Science of Campaigns," saying they identify "information warfare (I.W.) as integral to achieving information superiority and an effective means for countering a stronger foe." But it notes that neither document "identifies the specific criteria for

employing a computer network attack against an adversary," though they "advocate developing capabilities to compete in this medium."

It is a critique the Chinese could easily level at the United States, where the Pentagon has declined to describe the conditions under which it would use offensive cyberweapons. The Iran operation was considered a covert action, run by intelligence agencies, though many technques used to manipulate Iran's computer controllers would be common to a military program.

The Pentagon report also explicitly states that China's investments in the United States aim to bolster its own military technology. "China continues to leverage foreign investments, commercial joint ventures, academic exchanges, the experience of repatriated Chinese students and researchers, and state-sponsored industrial and technical espionage to increase the level of technologies and expertise available to support military research, development and acquisition."

But the report does not address how the Obama administration should deal with that problem in an economically interconnected world where the United States encourages those investments, and its own in China, to create jobs and deepen the relationship between the world's No. 1 and No. 2 economies. Some experts have argued that the threat from China has been exaggerated. They point out that the Chinese government — unlike, say, Iran or North Korea — has such deep investments in the United States that it cannot afford to mount a crippling cyberstrike on the country.

The report estimates that China's defense budget is $135 billion to $215 billion, a large range attributable in part to the opaqueness of Chinese budgeting. While the figure is huge in Asia, the top estimate would still be less than a third of what the United States spends every year.

Some of the report's most interesting elements examine the debate inside China over whether this is a moment for the country to bide its time, focusing on internal challenges, or to directly challenge the United States and other powers in the Pacific.

But it said that "proponents of a more active and assertive Chinese role on the world stage" — a group whose members it did not name — "have suggested that China would be better served by a firm stance in the face of U.S. or other regional pressure."

Table of Contents

Pentagon Warns North Korea Could Become a Hacker Haven

By Spencer Ackerman, WIRED, 03 May 2013

North Korea is barely connected to the global internet. But it's trying to step up its hacker game by breaking into hostile networks, according to a new Pentagon report.

"North Korea probably has a military computer network operations (CNO) capability," assesses the Pentagon's latest public estimate (.PDF) of the military threat from North Korea.

So far, suspected North Korean cyber efforts are more like vandalism and espionage than warfare — as with most so-called "cyberattacks" not related to the U.S./Israeli Stuxnet worm. But the Pentagon believes Pyongyang is going to lean into network attacks in the future, largely out of necessity.

"Given North Korea's bleak economic outlook, CNO may be seen as a cost-effective way to modernize some North Korean military capabilities," the report assesses. "The North Korean regime may view CNO as an appealing platform from which to collect intelligence."

North Korea appears to be feeling its way around in the dark of the internet and seeing what it can get away with. Since 2009, the Pentagon says, the North Koreans are believed to have targeted the servers of a major South Korean bank to erase customer records and render its online services inaccessible. Pyongyang likely DDOS'd a bunch of South Korean government and private websites over the last several years. Just last month, while tensions on the Korean Peninsula spiked, Seoul accused Pyongyang of infecting tens of thousands of computers used by the South's banking and television industries with malware.

Back in April, he website of the U.S. military command on the Korean peninsula briefly went offline — and fueled suspicion that Pyongyang was to blame. Interestingly, the Pentagon stops short of blaming North Korea for the outage.

All this is commensurate with what the Pentagon sees as a broader pattern in North Korea's military development: developing its unconventional prowess — like nuclear weapons and experimental long-range missiles — to compensate for its aged, creaking conventional forces.

North Korea has one of the largest arsenals on the planet. It's got a military of 950,000 personnel, mostly ground forces; 8,500 field artillery pieces; 4,100 tanks; maybe 100 short-range missile launchers; and more, mostly pointed at Seoul. But a lot of that stuff is decrepit crap, according to the Pentagon report.

Its most capable combat aircraft? Creaky MiG-29 and MiG-23 fighters. Its most recent aircraft acquisition? 1999, when it bought MiGs from — wait for it — Kazakhstan. The primary air tool to transport its (legitimately formidable) special-operations forces? "1940s vintage single engine, 10-passenger, bi-planes." Its surface naval fleet? "Primarily of aging, though numerous, small patrol craft." Most of Pyongyang's conventional weapons haven't been updated or upgraded since the 1970s.

The Korean People's Army "fields primarily legacy equipment, either produced in, or based on designs of, the Soviet Union and China, dating back to the 1950s, 60s and 70s, though a few systems are based on more modern technology," the report finds.

There are some major exceptions. Pyongyang's air-defense systems are upgraded relatives of Russia's intimidating S-300 system. It's going full speed ahead with efforts at an intercontinental ballistic missile. Its submarine fleet is one of the world's largest. Kim Jong-un is down with Dennis Rodman.

Significantly, the report does not back up a recent Defense Intelligence Agency assessment that North Korea might — might — be able to mount a nuclear warhead atop its missiles. The report says the North's working on it, not that it's shrunk a nuke down to sufficiently small size.

But even with the North's longstanding its "Military First" national strategy, its paltry economy doesn't provide Pyongyang with enough money to upgrade and modernize. Hence the emphasis on nukes — and network intrusions.

"North Korea has invested in a modern nationwide cellular network," the report notes. "Telecommunication services and access are strictly controlled, and all networks are available for military use, if necessary."

Table of Contents

Loose Lips: Candid Camera Club Alerts N. Korea of USS Nimitz's Arrival

From Fox News, May 8, 2013

It wasn't a tapped phone, a hacked computer or a double agent that tipped off North Korea that the U.S. Navy's biggest and baddest aircraft carrier was steaming toward the peninsula -- it was a perfectly innocent bunch of shutterbugs.

When Pyongyang's state-run media agency mentioned the ship's itinerary in a news release, a day before it was first reported in the South Korean media, alarm bells went off, according to the South Korean newspaper The Hankyoreh. U.S. and South Korean military officials initially feared a phone tap, intelligence leak or hacked email account might be to blame, according to South Korean media reports.

But it turned out that on Saturday night, a Seoul-based camera association known as the "O" Club had told its members that an aircraft carrier would berth in Busan on May 11, and that people were needed to drive American sailors around, a South Korea Ministry of National Defense said.

"… looking for two Busanites who can drive and speak basic English," read the message, posted on a photography website. "A U.S. naval aircraft carrier is coming on the 11th and leaving on the 13th, and you would just need to transport the U.S. sailors. Pay is 110,000 won ($101) a day. Two people wanted. Send a message if you're interested."

Another post offered suggestions on where to get good pictures of the massive ship. Someone in North Korea saw the ad and did some low-risk intelligence gathering.

Although neither post named the ship, officials believe North Korea were able to put together the details using other information already made public, including a post on the U.S. Navy's website last week that said the nuclear-powered Nimitz had entered the jurisdiction of the 7th Fleet, a South Korean Ministry of Defense official said Wednesday.

The U.S. and South Korea are staging anti-submarine exercises this week, and the Nimitz will participate in another joint naval exercise next week. Although the exercises come as tensions are rising between North and South Korea, officials publicly sought to downplay the Nimitz's appearance.

"We are not trying to deliver any message to North Korea with this exercise," a spokesman for the South Korea Joint Chiefs of Staff said, referring to this week's anti-submarine drills. "This exercise is for improving the U.S.-South Korean war-fighting power."

North Korea has vowed immediate countermeasures if even one shell fired during the joint U.S.-South Korea exercises lands in North waters.

The U.S. and South Korea are trying to push “the present state of war to an actual war,” according to a statement posted on the North’s government-run Korean Central News Agency website.

Table of Contents

Why Two Domains Are Better Than One

By John Knowles, E-crow newsletter, 9 May 2013

In recent weeks, the long-running discussion regarding exactly how the electromagnetic (EM) and cyber environments relate to each other has come back to the forefront with several voices calling for what appears to be the establishment of a single Cyber-EM environment.

The most prominent of these was Chief of Naval Operations ADM Jonathan Greenert. Building on his earlier articles about the Cyber and EM environments published in Naval Institute’s Proceedings magazine, Admiral Greenert contributed an op-ed piece for AOL Defense titled, "Wireless Cyberwar, the EM Spectrum, and the Changing Navy." He followed up what has been an exceptional effort to raise awareness of the EM environment by citing some excellent examples of the Navy’s growing dependence on the EMS, the need to "improve our awareness of the EM and cyber environments," and the Navy’s desire to "employ agility in the EM spectrum and cyberspace."

However, the concept at play seemed to be one of EM and cyber as a single environment. "With wireless routers or satellites part of almost every computer network, cyberspace and the EM spectrum now form one continuous environment," Greenert wrote.

As current events further push EM and cyber concerns forward, the number of voices calling for their consideration as one environment has grown. Though it appears to make sense on the surface, deeper consideration of the DOD’s broad operational responsibilities in the electromagnetic spectrum (EMS) make a combined Cyber-EM domain something that should be reconsidered before the Navy or any Service goes too far down that path.

UNDERSTANDING THE EM-CYBER RELATIONSHIP

Recent discussion has focused on an important concept – the evolving relationship between the cyber environment and the EM environment. (If you want, you can substitute the word "domain" for "environment," as JED often does.) But what is frequently described as a single Cyber-EM environment is really two separate environments – the cyber environment and the EM environment. To understand why this is true, it is worth taking a closer look at the characteristics of the cyber and EM environments.

Cyberspace, according to the DOD’s Joint Publication 3-12, is "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems and embedded processors and controllers." This means that cyberspace is not a natural physical environment. Cyberspace comprises man-made technologies and forms a portion of the information environment. This makes cyberspace very different from the EM environment.

The EM environment is a natural physical maneuver space that we visualize through the concept of the EM Spectrum (EMS). In this sense, the EM environment is like the Air, Land, Sea and Space domains. As a natural physical maneuver space, the EM environment (or operationally speaking, the EM Domain) cannot "merge" with another environment any more than the Air and Sea domains can converge to form a single Air-Sea environment or the Space and Cyber domains can converge to form a Space-Cyber environment. It just doesn’t work that way.

CONVERGENCE – A POWERFUL BUT MISAPPLIED TERM

In technology-heavy disciplines like electronic warfare (EW) and cyber operations, it is tempting to cite technology-related examples as evidence of a continuous Cyber-EM environment. There are numerous EM systems (jammers, radars and communications systems) that are networked via cyberspace. Cyber systems are also increasingly using the EMS via wireless networks. This trend is a type of technological convergence. (Many argue that "technological convergence" isn’t even the correct term for this trend and that "technology sharing" is a more accurate description.) The problem arises when we try to extend the significance of this trend beyond technology and argue that the cyber and EM environments are converging.

First of all, technology does not determine or define a natural physical maneuver space like the EM environment. The EM environment has existed from the moment of the Big Bang which is certainly long before humans began exploiting it for radio communications, radar, GPS, etc. Whatever tools the DOD uses to

maneuver within the EM environment, those technologies do not define the environment. The same rule is true for the information environment, of which cyberspace forms a part. More importantly, there is no relationship between EM and cyber technological convergence and convergence between the EM and cyber environments. Just as technology cannot define a domain, technological convergence cannot drive domain convergence.

When technological convergence has occurred in the past, it has not driven convergence between warfighting domains because physical environments cannot converge. Did the development of the aircraft carrier in the last century mean the naval and air environments were converging because we were flying planes from ships? Obviously not. Even though military aviation was a relatively new idea at the time, the Air and Sea domains were understood well enough for military leaders to know that the two could not form one continuous Air-Sea environment just because of technological innovation.

Or try looking at the putative Cyber-EM convergence theory in another way. If we take the cyber and EM technologies out of the equation, is the term "convergence" a good description of the Cyber-EM relationship? It is worth noting that no one in the DOD was arguing that the cyber and EM environments formed one continuous environment until after wireless data communications and software-defined radars and radios started to appear in the battlespace.

CYBER SYSTEMS ARE BECOMING MORE DEPENDENT ON THE EMS

If cyber and EM convergence isn't really what is happening, then what is happening between cyberspace and the EM environment? To answer that question, let's look at some historical examples in naval warfare.

During the early part of the last century, we began developing technologies that enabled our weapons systems to exploit the EM environment. In naval warfare, for example, ships began using radios before World War II. Then radars came into use. In the 1950's, we developed RF- and IR-guided missiles. Soon afterward, we developed electronic warfare systems to detect and defeat RF- and IR-guided anti-ship missiles. Ships then began to use satellites for navigation, weapons targeting and data communications. IFF systems evolved, too. What was happening was simple: ships – and by extension, naval warfare – was becoming more dependent on the EM environment. Yet no one was arguing that the naval environment was "converging" with the EM environment.

For the past 100 years, the same trends have been emerging in other warfighting environments. Air warfare has become dependent on the EM environment. Land warfare has become dependent on the EM environment. Space operations are extremely dependent on the EM environment. Throughout this period of growing EM dependence, no DOD leader has characterized this trend as "convergence" or called for a single Air-EM environment or Space-EM domain.

Now, let's look at cyber warfare. Over the past decade, cyber networks have become increasingly dependent on access to the EM environment, as they evolved from "wired" to "wireless" architectures. Like the other warfighting environments, this EM dependence is the true essence of the Cyber-EM relationship. It is worth noting here that while cyber operations are becoming more dependent on access to the EM environment, the opposite is not true. Most of the systems and devices that use the EM environment, as well as the EW systems that provide EM control, are not inherently dependent on cyberspace. Whether or not an EM system has access to cyberspace, that access does not enable their ability to maneuver in the EM environment.

From an EM environment perspective, cyber systems reside strictly in the "data transport" layer. Even potential or prospective cyber attacks delivered by RF jammers are essentially performing a communications function – delivering software code into a victim system – as opposed to a jamming function. For the most part, cyber systems are simply EMS "users" (just like radars, radios and GPS receivers), because data networks need access to the EM environment to move information around the battlespace. Their increasing use of the EM environment does not constitute convergence. Rather it demonstrates EM dependence, which is the true nature of the Cyber-EMS relationship.

The reason many in the DOD do not understand this relationship is because the DOD has spent the past 20 years building a network-centric fighting force. This focus on net-centricity has skewed much of the DOD's thinking around computers and networks to the point that cyber technologies have been endowed with significance well beyond their true importance. It is time to return to a more rational understanding of maneuver space, operational responsibilities, mission and technology with regard to the EM environment and the cyber environment.

THE NEED FOR AN EM STRATEGY

Over the years, JED authors, such as John Clifford, Jesse "Judge" Bourque, Col Jeff Fischer and others, have explained why the DOD needs to understand that the EM environment is a unique maneuver space upon which all of the other warfighting domains – Air, Land, Sea, Space and Cyberspace – depend.

The EM environment is vast, and the DOD must maintain operational responsibility for all of the parts it needs to use, manage and control. The DOD cannot afford to build most of its EM strategy around those small portions of the EM environment that support cyber-centric or network-centric operations while pushing the vast majority of its EM responsibilities to the outer edges of this strategy. Instead the DOD needs a strategic focus that covers the whole EM environment all of the time because it is using ever larger portions of this EM maneuver space. As the US Army discovered when Iraqi insurgents began using radio-controlled improvised explosive devices (RCIEDs), an adversary will always seek to exploit areas of the EM environment where the DOD yields operational control.

The best way to prevent this from happening again and again in the future is for the DOD to recognize that it needs a comprehensive strategy for the EM environment – one that integrates EM use, EM management and EM control. Many of the "piece-parts" needed for this strategy already exist. Some areas, such as EM management and electronic warfare, are even beginning to coordinate more effectively. This is a step in the right direction. But the DOD needs to do a lot more, and the first step is to recognize that it needs a better strategy for the EM environment.

Table of Contents

The Problem with Crowdsourcing Intelligence in Syria

By Thomas Chappelow, DefenceIQ, 05/09/2013

In December 2010, a series of protests in Tunisia gave birth to what is now dubbed the Arab Spring. The events that followed have been studied in-depth, attracting a large volume of commentary. Interestingly though, there is little talk about the use of crowdsourcing to gather intelligence. This is especially curious considering that information collected in this way has formed the backbone of what we know about the uprisings.

This is nowhere more apparent than in Syria, where for perhaps the first time in history ordinary citizens are able to use social media to blog and photograph human rights abuses connected to the conflict. More importantly however, they also document the movement and tactics of security forces; creating an environment in which they are largely able to stay ahead of government plans, effectively paralysing the state military during offensives.

Rebels are blogging, tweeting, mapping and photographing every single detail of the civil war, creating an unprecedented mountain of information that can be farmed for actionable intelligence by both the protesters and foreign intelligence agencies.

Why crowdsourcing?

America, amongst others, recognises that the civil war has turned Syria into a regional tinderbox, attracting thousands of foreign mujahideen; many of whom pose a serious threat to Western interests in the middle east.

The current problem facing policy chiefs in Washington is that they do not have a clear understanding of which opposition groups to trust; which are acceptable to the West; and which will have a part to play in Damascus long after hostilities have ceased.

This in part can be attributed to the lack of authenticated human intelligence (HUMINT) coming from inside Syria. With the closing of the U.S. embassy – taking with it the CIA station – there are few traditional sources left.

The Assad regime's refusal to allow foreign journalists access to the country only serves to compound the issue by closing off a vital flow of information. Of course there are exceptions, but these are limited.

I would note that the British and French embassies are still functioning, and receiving a slightly broader view of events on the ground. Although the signs are that this is mainly due to a couple of Syrian army defectors passing information to embassy officials, but the intel does not offer any major advancement on what we already know.

Other methods that have played a vital role in recent intelligence operations, such as the use of communications interception and satellite imagery to track the movements of security forces in Libya, are now of little use. This is mainly because Syrian military radio traffic follows the strict Russian COMSEC principle of 'radio silence', and any chatter that does appear on the net increasingly appears to be misinformation.

Whilst it can be said that satellite imagery has provided some evidence of troop movements and shelling, those images do little to add to the West's policy playbook here. This is because the issue at hand is not whether Assad is attacking civilians and opposition forces (nobody disputes this), but rather which, if any, opposition forces should be supported.

This means that with a lack of traditional sources to rely on, the global intelligence community has to look elsewhere for its information – and for intel-starved policy makers, crowdsourcing appears a juicy prospect – until it goes wrong.

Where crowdsourcing falls short

Last week the Obama administration declared it had seen evidence of Sarin use by the Assad regime. But just a few days later Carla Del Ponte of the U.N. commission, the organisation that is investigating human rights abuses in Syria, suggested she had 'concrete suspicions' that the gas was in fact used by opposition fighters. And whilst the commission was keen to stress that no formal conclusions have yet been reached, it does call into question the legitimacy of intelligence claiming the gas had been deployed by the regime.

The apparent problem with the intelligence seen by U.S. agencies was that it came from opposition groups, via other opposition groups, who had gathered the information and evidence from anonymous actors both inside and outside of Syria.

Putting aside the fact that opposition groups have a vested interest in attracting foreign military assistance, as yet nobody seems to know who those anonymous actors are. Indeed it is widely accepted that there are multiple extremist groups fighting in Syria, with the most prominent being the Al-Nusra Front who recently pledged allegiance to al-Qaida.

Using intelligence gained from crowdsourcing that could have originated with extremist groups is a very dangerous road to walk. But frankly there are limited options for analysts when faced with such a mountain of information, knowing very little of which can be verified, but having the acute knowledge that there is a desperate shortage of other traditional sources.

In fact the principles of crowdsourcing intel are a direct contradiction of the US Army's definition of human intelligence gathering which says, "the collection of information by a trained human intelligence collector from people and their associated documents and media sources to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities." (FM3-24, 2006, 3-26)

The point this manual makes is that anyone can receive voluntary information from a 'walk-up' or anonymous source, but conventional military and agency doctrine commands that only qualified collectors may gather intelligence from designated human sources – and by designated they mean trusted.

This is where crowdsourcing falls short; it is incredibly difficult to trust information that has no documented or vetted origin. And there are many examples of it falling short of the standard expected of intelligence used to develop foreign policy. This was most recently shown in the aftermath of the Boston Marathon bombings where at least four people were wrongly accused of being the suspect, one of whom has later been found dead.

Who is benefitting?

The question of who has the most to gain from the intelligence black-hole in Syria has a simple answer: both sides have the ability to benefit from the lack of traditional sources, but it is the opposition activists tasked with building international support for intervention who will benefit the most, easily manipulating evidence and injecting it into the twittersphere, knowing that eventually it will land on the desk of an agency officer. And unless there are intelligence service boots on the ground, that officer would have a hard time authenticating it.

I am not saying that a large chunk of reports from inside Syria are incorrect, it is well known that the daily killing of civilians is widespread, unjust and a clear breach of international law; but one cannot ignore the fact that opposition groups are growing increasingly desperate to gather foreign support, arms and funding – misinforming the social web is the least of their worries.

Table of Contents

US Government Becomes 'Biggest Buyer' Of Malware

By Zack Whittaker, Zero Day, May 13, 2013

The U.S. government has become the biggest buyer of malware, according to a Reuters special report, which is leading to growing concerns in the technology and intelligence industry.

By engaging with a dubious, unregulated grey market of hacks, vulnerabilities, and exploits, which the federal government can use to strike back at its opponents that in turn attack it, some are warning that Washington's actions are "encouraging" hacking and similar practices.

The security industry is concerned that the superpower is failing to register the vulnerabilities it buys, funded by the taxpayer, because it is instead using the exploits to attack and infiltrate foreign networks in order to lay cyberweapons and spy technology.

This "offensive" cybersecurity strategy is leaving ordinary U.S. businesses and consumers vulnerable to their own security breaches and hacks, according to former White House cybersecurity advisors Howard Schmidt and Richard Clarke.

"If the U.S. government knows of a vulnerability that can be exploited, under normal circumstances, its first obligation is to tell U.S. users," Clarke said.

Meanwhile, Schmidt, the former White House cybersecurity coordinator who retired from the Obama administration in May last year, said it is "pretty naive" to believe that when a zero-day flaw is discovered, they are the only person in the world who knows about it.

"Whether it's another government, a researcher, or someone else who sells exploits, you may have it by yourself for a few hours or for a few days, but you sure are not going to have it alone for long."

Because the government relies on flaws in existing networks, software, and systems, the argument is that these hacks and exploits would be less effective if the security industry informed the public of such threats, which would alert companies to patch their software and networks in order to prevent such attacks.

"So the more the government spends on offensive techniques, the greater its interest in making sure that security holes in widely used software remain unrepaired," said Reuters.

It comes in recent weeks after The New York Times reported that the Obama administration can order a pre-emptive cyberattack against a threatening nation if the U.S. needs to defend itself. Ultimately, the order would have to come from the president himself.

The Times' report noted that as a result of Obama's victory in taking a second term in the White House, his administration is reviewing the range of cyberweapons that the U.S. government has in its possession.

These cyberweapons are not necessarily powered-up datacenters that launch denial-of-service (DoS) attacks against foreign machines, or specially crafted malware designed to infiltrate the networks of oppressive regimes; Stuxnet was just one of a few malware attacks found in the wild by private research firms.

Many such cyberweapons, in fact, can fit on an ordinary USB thumb drive. Many can be sent via email. And some are no different from the viruses and exploits that black-hat hackers use against unsuspecting citizens going about their daily business.

Such exploits can be sold for as little as $50,000, which is small change to the U.S. government, but many are toward the $100,000 price mark for a number of exploits that are needed for a "solid operation."

"Exploits are used as part of lawful intercept missions and homeland security operations as legally authorized by law," according to Paris, France-based Vupen, which spoke to Reuters. Vupen began selling vulnerabilities to governments and intelligence agencies when software makers failed to agree on a compensation system. The security firm said it sells its discoveries as part of efforts to "protect lives and democracies against both cyber and real-world threats."

Vupen first came to prominence when it was named as part of a Wikileaks release in late 2011 of 287 initial documents describing internet and cell-phone based technology procured by "dictatorships and democracies alike," first developed by the U.S., the U.K., Australia, and Canada.

The security company was named as a company that manufactures trojan malware that can hijack computers and phones — including BlackBerrys, iPhones, and Android devices — that can be used to record movements, sights, and sounds in the rooms they are located in.

Table of Contents

How Twitter Is Messing With Al-Qaeda's Careful PR Machine

By Tony Busch, the Atlantic, 14 May 2013

The idea that the Internet facilitates Al-Qaeda's recruitment and messaging campaigns is not new. However, more than ever, the changing landscape of the online environment is allowing for dissent from within the ranks of Al-Qaeda's supporters. Gone are the days when Al-Qaeda's senior online ideologues could control the flow of information by operating their own bulletin board-style forums. While Al-Qaeda and its supporters still facilitate discussion through their own web communities, the nature of jihadi discourse today is much more democratic, with jihadi personalities claiming inside knowledge dispersed across the online environment. The evolution toward platforms such as Twitter that empower the individual are allowing Al-Qaeda's supporters to

avoid forum censors and promote their own personal narratives, which are not necessarily in agreement with that of Al-Qaeda's messaging strategy writ-large.

This phenomenon was at center stage in early April when Al-Qaeda's affiliate in Iraq (AQI) committed an unthinkably reckless strategic messaging error. On April 9, AQI announced the incorporation of Jabhat Al-Nusra in Syria into an AQI-administered Islamic state aspiring to govern Iraq and Syria. Effectively, AQI attempted to define Al-Nusra as no more than a subordinate to AQI. Al-Nusra, one of the Syrian opposition's most effective fighting groups and indisputably Al-Qaeda's most popular affiliate, was quick to respond. Just one day later, they denied knowledge of the merger and professed a direct pledge of loyalty to Al-Qaeda senior leader Ayman Al-Zawahiri. Despite the State Department placing Al-Nusra on it list of foreign terrorist organizations in December 2012, this was the first time that Al-Nusra's leadership had publically acknowledged their link to Al-Qaeda.

These events led to a flurry of debate on jihadi web forums that support Al-Qaeda. Many jihadists were quick to criticize AQI and began openly wondering how an affiliate of Al-Qaeda, a group that is notoriously careful in crafting its messages, could commit such a blunder. However, jihadi forum moderators suppressed commentary that criticized AQI, and the lack of free speech within Al-Qaeda's movement was unmistakable. Just several years ago it might have ended there without any serious repercussions, but today's is a different Internet environment. The rise of social media platforms championing the power of the individual has changed the online jihadi landscape. While the new model works to the benefit of Al-Qaeda so long as its proponents promote a unified message, the new reality also magnifies dissent.

Soon after Al-Nusra refuted the merger with AQI, one of the most widely trusted jihadi political analysts on Twitter attacked AQI's integrity as an organization. Abdullah bin Muhammad, as he identifies himself on his account (@Strategyaffairs), criticized AQI's decision to carry out attacks during a recent period of Sunni protests in Iraq, remarking that such actions "do not serve [anyone] but the Iranian enemy." Additionally, Abdullah bin Muhammad produced a document in which Ansar Al-Islam, an old AQI ally from the days of the resistance against the American forces in Iraq, listed crimes that AQI operatives allegedly committed against Ansar Al-Islam members. According to Abdullah bin Muhammad, Ansar Al-Islam asked him to intervene to end the feud. Armed with this information, Abdullah bin Muhammad alleged that unknown parties had infiltrated AQI and were attempting to translate that effort into influence over Al-Nusra in Syria. Such an open deviation from the prevailing AQI narrative on mainstream sites is historically very rare.

On a typical jihadi forum, Abdullah bin Muhammad's inflammatory accusations would not survive long before being deleted. But in the free market of ideas that is Twitter, where Abdullah bin Muhammad has over 35,000 followers, his comments were re-tweeted hundreds of times as Al-Qaeda junkies across the web discussed the spike in jihadist criticism of AQI. Additionally, agreement by Assad Al-Jihad2, a long-time online proponent of Al-Qaeda's global jihad whose articles have been published by official Al-Qaeda media sources and who is nicknamed "The Spearhead of the Mujahidin" by his followers, only placed more credibility on Abdullah bin Muhammad's allegations.

The ability of Abdullah bin Muhammad's Twitter accusations to travel far and wide was illustrated when his comments were re-posted on sites such as The Yemeni Council, a vibrant and largely moderate Arabic discussion forum where current events receive spirited debate and where Al-Qaeda supporters are actively attempting to win the hearts and minds of the site's mostly Yemeni participants. Feeling empowered by the legitimacy that comes with the endorsement of Abdullah bin Muhammad and Assad Al-Jihad2, a staunch supporter of Al-Qaeda on The Yemeni Council admitted to his own deeply held concerns about AQI's trustworthiness. Interestingly, this Al-Qaeda ideologue also expressed regret over making a statement so critical of AQI on a mainstream site, but remarked that he was sure that such a comment would not be welcome on a jihadi forum. As this post shows, the suppression of the allegations against AQI pushed Al-Qaeda's supporters' criticism into more moderate areas of the online social media environment, a development that is at best an embarrassment to Al-Qaeda.

It's clear that Al-Qaeda is increasingly less able to control the conversation by hosting it on its own sites and indoctrinating the participants to the point that they no longer dare to diverge from Al-Qaeda's lines of persuasion.

Today, some of the group's most successful online advocates, such as Abdullah bin Muhammad, Assad Al-Jihad2, and the plethora of Al-Qaeda sympathizers on Arabic web forums like The Yemeni Council, are making independent judgments about how to present Al-Qaeda's activities to the world. In this case, that process translated into a difficult decision: Al-Qaeda supporters either (1) amputated the disease-ridden limb that is AQI so that the larger Al-Qaeda body could flourish, or (2) remained steadfast behind an affiliate that has been a mainstay in the Al-Qaeda family for most of the last decade. At this early stage, it is difficult to know which faction is in line with Al-Qaeda's senior leadership, but certainly the two opinions are mutually

exclusive. Only time will tell as to how Al-Qaeda's old guard will respond to this and other debacles that result from jihadis going rogue on Twitter.

Table of Contents

Chinese University Lab Linked To PLA Cyber Attacks

By Bill Gertz, Washington Free Beacon, May 14, 2013

A computer science laboratory at China's Wuhan University has been linked by U.S. intelligence agencies to Chinese military cyber attacks on the West.

According to U.S. officials, the Key Laboratory of Aerospace Information Security and Trusted Computing at Wuhan's Computer Science School in central China's Hubei Province is the latest cyber warfare research and attack center to be identified from within China's secret cyber warfare program.

The Pentagon's latest annual report on China's military, made public last week, for the first time confirmed that Chinese cyber attacks on the U.S. government appeared "attributable directly to the Chinese government and military."

A report by the private cyber security firm Mandiant in February identified China's main military cyber espionage group near Shanghai as Unit 61398, part of the People's Liberation Army's 2nd Bureau of the General Staff Department's 3rd Department, known as 3PLA.

The Project 2049 Institute, a Virginia-based think tank, revealed a separate Chinese military cyberwarfare unit called the Beijing North Computing Center, also part of the 3PLA, four months before publication of the Mandiant report.

According to U.S. officials, the Key Laboratory, located about 425 miles west of the Chinese port city of Shanghai, is one of three computer science laboratories at the university. It was set up in 2008 and is considered one of the premier information security and cyber warfare centers at the university.

Wuhan's Computer Science School has trained more than 760 people who currently are in the Chinese military and government over the past decade.

The lab received funding from several Chinese military elements, including 3PLA.

Another Wuhan University computer science laboratory was identified by the officials as the Information Network Attack and Defense Research Center.

The Key Lab is noted for its development of unique computer warfare software platform called the SimpleISES Information Security Experiment System that is used in training and conducting cyber attacks.

The system can be used by 20 students at a time to conduct cyber attacks on networks. SimpleISES was developed by Beijing Simpleware Technology Co., Ltd. and is used at more than 30 universities throughout China.

Experts say the system is believed to be a key element in the massive Chinese-military related cyber attacks against the Pentagon and the U.S. government, as well as China cyber attacks in other nations.

Mark Stokes, a former Air Force officer and Pentagon specialist on China now with the Project 2049 Institute, said he was not familiar with the Key Lab. Stokes coauthored a 2011 report that revealed one of 12 3PLA operational bureaus is located in Wuhan.

"There are several of these kinds of state and defense labs," Stokes said in an email.

A computer security expert who asked not to be identified by name said Simple ISES "seems to be basically a teaching system for training hackers."

"If Wuhan is involved, then they are using the system to train next generation university students to be hackers," the expert said. "It seems that it is a modular to assist in the development and testing of new attacks."

The Pentagon's annual report, which was dismissed by Chinese government spokesmen as "groundless," stated that in 2012 "numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military."

"These intrusions were focused on exfiltrating information," the report said. "China is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs."

According to the Pentagon report, cyber attacks are aimed at information that could benefit China's defense and high-technology industry, as well as "policymaker interest in U.S. leadership thinking on key China issues,

and military planners building a picture of U.S. network defense networks, logistics, and related military capabilities that could be exploited during a crisis."

"Although this alone is a serious concern, the accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks," the report said.

China plans to use cyber warfare capabilities in future wars by primarily gathering data for intelligence and computer network attacks.

Additionally, cyber warfare attacks will be employed to limit enemy action or slow military responses "by targeting network-based logistics, communications, and commercial activities," the report said.

Cyber warriors also will be coupled with conventional military attacks as a "force multiplier" during war or crises, the report said.

The Pentagon report said Chinese military writings contain extensive reports on cyber warfare doctrine. Two key writings were identified as "Science of Strategy," and "Science of Campaigns," which outlined how to achieve "information superiority" in warfare that would allow a weaker power to defeat a stronger foe.

"China's military continues to explore the role of military operations in cyberspace as a feature of modern warfare and continues to develop doctrine, training and exercises which emphasize information technology and operations," David Helvey, deputy assistant defense secretary for East Asia, told reporters in releasing the report May 6.

Zhang Huanguo, an official involved in the laboratory, did not return emails seeking comment.

In addition to Zhang, other Chinese who are part of the Key Lab include Lina Wang, who heads the unit, Du Ruiying, and Fu Jianming, who is known to be involved in information attack and defense activities.

Zhang is considered the liaison with the People's Liberation Army (PLA). The Key Lab in the past received funding from the PLA Information Engineering University, the General Staff Department Confidential Bureau, and the 3PLA.

The PLA Unit 61478, a secret cyber warfare unit, provided other funding for the lab.

Table of Contents

China Conducts Test of New Anti-Satellite Missile

By Bill Gertz, Washington Free Beacon, 14 May 2013

China's military on Monday conducted the first test of a new ground-launched anti-satellite missile that was fired into space and disguised as a space-exploration rocket, according to U.S. officials.

The test was carried out early Monday from the Xichang Space Launch center and was identified by officials as the new Dong Ning-2 ASAT missile.

The ASAT test comes a week after China protested the release of the Pentagon's annual report on the Chinese military buildup that mentioned Beijing's development of anti-satellite weapons.

The Free Beacon first disclosed the existence of the new missile in October and a missile researcher reported in January that a new ASAT missile was being readied for its first test.

Chinese Foreign Ministry spokesman Hong Lei was asked if China conducted an ASAT test during a briefing for reporters in Beijing on Monday. He did not deny that it was carried out. "I am not aware of the development that you described," he said. "China has consistently advocated the peaceful use of outer space and is opposed to militarizing and conducting an arms race in outer space."

A Pentagon spokesman had no immediate comment.

A U.S. official familiar with intelligence reports said the DN-2, as a high earth-orbit attack missile, is a significant advance for China's program of developing asymmetric warfare capabilities for use against the United States. Others include cyber-warfare capabilities and anti-ship ballistic missiles.

It could not be learned if the latest ASAT test involved an impact with a target satellite.

A second official said the Chinese apparently disguised the ASAT missile test as a space exploration experiment. The website of the National Space Science Center, part of the Chinese Academy of Sciences, reported Monday that a sounding rocket was used in a high-altitude scientific exploration test.

"This experiment used a high-altitude space-exploring rocket, Langmuir probe, high-energetic particle detectors, magnetometers and barium-powder release experimental apparatus and other payload of scientific exploration to test and measure the ionosphere, the high-energy particles and magnetic fields of the near-Earth space strength and structure," the notice said.

China in 2007 conducted its first successful hit-to-kill ASAT test against a weather satellite in low-earth orbit. The impact left tens of thousands of pieces of debris in orbit that continue to threaten both manned and unmanned spacecraft.

Defense officials have said China's ASAT weapons, including missile interceptors, lasers, and electronic jammers, are designed to disrupt satellite communications and navigation systems used extensively by the U.S. military in conducting joint warfare.

Defense Secretary Chuck Hagel stated in written answers to questions during his confirmation hearing in January that the United States would seek to avoid engaging in hostilities in space.

However, Hagel revealed that U.S. space policy calls for "the secretary of defense to develop capabilities, plans and options to deter, defend against, and, if necessary, defeat efforts to interfere with or attack U.S. or allied space systems."

The statement was the clearest indication that the Pentagon is preparing to develop "counterspace" weapons in response to Chinese anti-satellite weapons.

"The chances are good this is indeed an ASAT test as it was launched from the Xichang Space Launch Center, the same launch site used for the January 2007 successful SC-19 ASAT interception of a Chinese weather satellite," said Rick Fisher, a senior fellow at the International Assessment and Strategy Center. Xichang is located in southern Sichuan Province.

Fisher said Chinese Internet reports stated that the ASAT test of what U.S. official say was a DN-2 may have up to four stages and included one or two liquid-fueled upper stages to provide greater thrust as the missile closed in on a target.

"While there so far has been no report of a successful interception, even a very near miss would serve to validate this new [People's Liberation Army] ASAT system," Fisher said.

A validated DN-2 ASAT system would provide the Chinese military with the capability to "degrade or severely damage the U.S. Global Positioning Satellite (GPS) system," he said.

"This is not merely a threat against some American military satellites, but a threat to a what has become a vital part of the global electronic infrastructure, affecting global commerce and financial flows, to your personal finances that contribute to personal freedom."

Fisher said China has been "preaching" that other states should disarm while Beijing secretly builds space weaponry at the same time it has denied being engaged in the space arms buildup.

"In the face of such a threat, the United States simply has no choice but to pursue symmetric capabilities to deter Chinese attacks in space, but also to consider its own requirements for space superiority," he said.

The major concern for Pentagon war planners is that China, with an arsenal of around two dozen anti-satellite missiles, could severely disrupt U.S. command-and-control systems, intelligence-gathering satellites, and navigation satellites used to guide precision guided missiles.

Security analyst Gregory Kulacki said in an online posting in January that the ASAT test was expected as early as that month.

"Given these high-level administration concerns and past Chinese practice, there seems to be a strong possibility China will conduct an ASAT test within the next few weeks," Kulacki, a Chinese-language speaker with the Union of Concerned Scientists stated.

Defense officials disclosed to the Free Beacon that the DN-2 test was initially planned for last fall, but was delayed by the Chinese over concerns that the test would upset President Barack Obama's reelection bid.

While details of the DN-2 are not know, U.S. officials said it is expected to be a high earth-orbit interceptor capable of destroying strategic navigation, communication, or intelligence satellites by ramming into them at high speeds.

The DN-2 is said to be capable of hitting targets in high-earth orbit between 12,000 and 22,236 miles above earth. Many military, intelligence, and commercial satellites orbit at that altitude.

A Pentagon-State Department report to Congress last year on export controls stated that in addition to ground-launched ASAT missiles, China is building high-technology kinetic and direct energy weapons for ASAT use.

Table of Contents

New Payload Brings Jamming Capability To An Army UAS For The First Time

By Defense Systems Staff, May 14, 2013

Raytheon has delivered two electronic attack payloads for use on the Army's MQ-1C Gray Eagle unmanned aircraft system, which will mark the first time the Army will have jamming capability on a UAS.

The payload was developed in support of the Army's Networked Electronic Warfare, Remotely Operated (NERO) system, and delivered as part of a contract awarded by Navy NAVSEA-Crane in 2012. NERO is utilized on the Gray Eagle as an airborne electronic attack system capable of providing beyond-line-of-sight jamming capability to support ground troop operations.

The NERO system builds on the Army's Communications Electronic Attack with Surveillance and Reconnaissance (CEASAR) program. By migrating the same pod system and advanced capability to the Gray Eagle, NERO is capable of two- to three-times longer missions with reduced operating costs compared to it's current application on a manned twin-engine Beechcraft King Air C-12 aircraft, according to Raytheon. CEASAR was first awarded in 2010.

"NERO provides critical jamming capabilities to warfighters in counterinsurgency environments," said Glen Bassett, director of Advanced Communications and Countermeasures for Raytheon's Space and Airborne Systems business, in a press statement. "We leveraged our combat-proven success from the manned CEASAR program to deliver this key tactical electronic attack capability onto an unmanned application."

Table of Contents

Communication Systems Subject To Monitoring, OPSEC Reminders

By Staff Sgt. Christopher Gross, 460th Space Wing Public Affairs, 5/6/2013

5/6/2013 - BUCKLEY AIR FORCE BASE, Colo. -- Some of Team Buckley members have been informed of operational security violations, due to a no-notice monitoring period by the 67th Network Warfare Wing, Lackland Air Force Base, Texas.

The 67th NWW can intercept email that includes critical information list and other attachments containing personally identifiable information. Some examples of these include recall rosters, documents containing passwords and enlisted performance reports.

Violations are detected through the Telecommunications Monitoring and Assessment Program, which can scan mail for any type of attachments or key words.

"TMAP isn't something that just started," said Gretchen Myers, 460th Space Wing operation security program manager. "We've been aware of it; we just weren't getting pinged on it."

The discrepancies that are being reported aren't because of any guidance that hasn't been put in place. Sending documents or email which contains PII or CIL from a government network to a personal account has never been allowed, according to Capt. John Robinson 460th SW Plans and Programs deputy chief.

"The reason they do this, (is because personal accounts) are unprotected systems," Robinson said. "(Adversaries) can take it and use that information against you, against the government. People shouldn't be sending this stuff. That's how identities get stolen."

Violators of the policy are subject to discipline, the severity of the discipline is determined on a case-by-case basis. It can range anywhere from some refresher training to an investigation involving the member's chain of command.

Government phones, portable electronic devices and computers are all subject to being monitored at any time. Air Force Instruction 10-712, TMAP, explains in detail what is subject to monitoring.

According to Myers, members don't only need to be aware of what's being sent in email, but there are also several other preventative security measures people can do daily. This includes the bases' 100 percent shred policy. Myers said several files have been found in dumpsters containing PII.

"We continue to find stuff in the dumpsters. It's stuff with account number, social security numbers, EPRs, things people probably don't want us to see," she said.

Members should also be aware of what's being posted on social media sites. For example if someone is going on leave and the location and duration is posted to a social media site, this opens up vulnerabilities for adversaries to take advantage of.

The same applies to out-of-office replies. No exact days or location should be included in the reply. Only that the member is out of the office and a point of contact to assist the customer.

Table of Contents

US Could Use Cyberattack on Syrian Air Defenses

By Jim Michaels, USA Today, 16 May 2013

WASHINGTON – The Pentagon has cyberattack capabilities that allow the U.S. military to help blind Syrian air defenses without firing a shot, according to military analysts.

"One of the reasons the Air Force has paid so much attention to cyberwarfare is ... for beating enemy air defenses," said James Lewis, an analyst at the Center for Strategic and International Studies.

U.S. abilities to defeat Syria's air defenses are central to a debate over whether to intervene in the 2-year-old civil war. Electronic methods to disable enemy air defense systems include the injection of malware, a form of computer software, into the air defense network through a computer attack or by traditional electronic warfare aircraft capable of jamming radar.

The radars act like wireless transmitters and jammers can send false or destructive information into the radar, which then gets into the network, said Shlomo Narkolayev, an analyst who previously worked on cyber issues for the Israeli military's Unit 8200, which handles cyberwarfare.

"It's not hard to do this," Narkolayev said.

Syria and other nations are constantly adjusting the electronics for their air systems, and Air Force documents show the U.S. military does the same with its cyberweapons. They are constantly updated to counter changes made by enemy militaries.

A 2007 Israeli attack on a suspected Syrian nuclear power plant in 2007 provided a template for a future attack. The Israelis used a cyberattack to disable Syrian air defenses before aircraft entered Syrian airspace.

The Israeli attack was a quick strike that only required temporarily blinding air defenses. Establishing a no-fly zone would be a lengthier campaign that would require taking down Syrian air defenses for weeks or months.

Cyberattacks can cause permanent damage, Lewis said. U.S. forces have been reluctant to use cyberattacks for fear of creating collateral damage from malware that could damage other networks and because of concerns that enemy nations will copy the destructive malware once it is released. "We've been very cautious with the use of cyberweapons," Lewis said.

The Pentagon is in the process of reviewing new rules of engagement for cyberwarfare.

Syrians could take the system offline to avoid an infection spreading, but then the system would be less effective, Lewis said.

The Pentagon has said any air campaign would be a challenge because of the size and sophistication of Syrian air defenses, which are far more extensive than in Libya, where the United States and NATO created a no-fly zone in 2011.

"It's a much denser and more sophisticated system," Army Gen. Martin Dempsey, chairman of the Joint Chiefs of Staff, said recently.

U.S. and allied aircraft successfully launched an air campaign in Libya that helped defeat the regime of Moammar Ghadafi. It has frequently been help up as a model of what to do in Syria.

The White House launched an initiative to provide non-lethal aid to rebels battling the regime of Syrian President Bashar Assad, but has not decided on any further military options.

The question of how to respond has taken on renewed urgency after the Obama administration said the Assad regime has probably used chemical weapons.

Critics of the White House's Syrian policy, including Sen. John McCain of Arizona, a leading Republican voice on foreign policy issues, advocate a more robust response, including establishing a no-fly zone.

While cyberwarfare provides some advantages it is not without risk and cannot replace more conventional tactics, said Jeffrey Carr, founder of Taia Global, a cybersecurity consultancy.

"Cyber is not a magic bullet," he said.

Analysts say if cyberattacks were used it would likely be alongside more traditional methods, such as jamming radar and missiles that lock on to radar sites. That requires pilots who risk their lives flying in dangerous airspace.

Air defense systems generally tie radar and missile sites together over a computer network. The system may be generally closed, but may connect with the Internet at junctures that are vulnerable to outside attack, analysts say. "Once you penetrate the systems you can do anything," Narkolayev said.

Table of Contents

GAO: Military Propaganda Efforts Flawed

By Tom Vanden Brook, USA Today, 24 May 2013

Washington -- Pentagon propaganda programs are inadequately tracked, their impact is unclear, and the military doesn't know whether it is targeting the right foreign audiences, according to a government report obtained by USA TODAY.

Since 2005, the Pentagon has spent hundreds of million of dollars on Military Information Support Operations (MISO). These propaganda efforts include websites, leaflets and broadcasts intended to change foreigners' "attitudes and behaviors in support of U.S. Government" objectives, according to the report by the Government Accountability Office. Some of them disclose the U.S. military as the source; others don't.

The Pentagon's response noted that it partly concurred with the GAO criticism. Lt. Col. James Gregory, a Pentagon spokesman, said Thursday the military is revising its tracking requirements for propaganda programs, has a pilot program to assess their effectiveness and will soon publish revised guidelines that emphasize better planning.

The report offers a rare glimpse inside the cloaked world of military propaganda, much of which is held secret by the Pentagon. It shows the effort extends from Southeast Asia to South America, with special operations troops deployed to embassies to "erode support for violent extremist ideologies."

The stakes are high. Used effectively, the programs can dampen extremism and increase support for U.S. military operations. However, "if used ineffectively, MISO activities have the potential to undermine the credibility of the United States and threaten (Pentagon) and other agencies' efforts to accomplish key foreign policy goals," the report says.

While the report says some of the military's propaganda teams have succeeded in the 22 countries, "it is unclear whether MISO activities are effective overall."

"Once again we are seeing a misguided spending approach by the government," said Scott Amey, general counsel of the non-partisan watchdog the Project on Government Oversight.

Military propaganda and marketing efforts have been the focus of a series of USA TODAY stories. In 2012, the newspaper found that the Pentagon had spent as much as $580 million per year on propaganda programs at the height of fighting in Iraq and Afghanistan but had trouble gauging their effectiveness. It spent $54 million last year, according to the GAO. The GAO refused USA TODAY's request for the report, which was obtained from another government source.

The GAO found three "weaknesses" in the Pentagon's tracking of its propaganda programs:

The Pentagon and Congress "do not have a complete picture" of the efforts and the funding used to pay for the programs.

The Pentagon can't measure the effects of propaganda programs well enough to know where to allocate funding.

Lacking goals, the Pentagon does not have "reasonable assurance" that it is putting resources into countries that need it.

Gregory noted that the Pentagon already provides Congress with substantial data on its MISO programs every three months.

The Pentagon "submits an exhaustive report of all MISO activities to key congressional staffers," Gregory said.

"This report, often well in excess of 100 pages, provides comprehensive tracking of all MISO activities and the resources used to support them."

The report also outlines how propaganda works. In war zones such as Afghanistan, the military deploys three- and four-soldier MISO teams to drop leaflets telling insurgents how to surrender, air radio broadcasts "to explain U.S. military operations in a favorable light," collect local propaganda and devise counterpropaganda, according to the report.

It also relies heavily on contractors to produce advertising, leaflets and radio broadcasts, many of them unattributed to the U.S. government because locals do not trust western influence, senior military officerstold USA TODAY last year.

In safer countries, teams of two to 10 special forces soldiers are deployed at the request of combatant commanders and ambassadors. They lead programs that include helping "instill confidence by local populations in their law enforcement" and offering rewards for information.

Senior State Department officials told GAO that the efforts were valued at embassies. In Bangladesh, for example, the team worked with the U.S. Agency for International Development and "another (Pentagon) organization" to incorporate counter-radicalization messages into disaster response exercises." In Peru, a top-level Drug Enforcement Administration official praised a military team for its effort in the battle against "Shining Path" terrorists.

Less successful: regional websites set up by the military. U.S. Special Operations Command provided $22 million for combatant commands, such as Central Command in the Middle East, to operate regional websites "that offer readers an alternative to extremist ideology." They're "an important tool," according to the Pentagon, but GAO found "instances where the websites are not well-coordinated" with local embassies or even MISO teams in those countries.

In Nepal, for example, the embassy's public affairs office was "unaware of U.S. Pacific Command's website." State Department officials have expressed concern about U.S. Africa Command's website "about the Maghreb region of northern Africa, saying that a program marketed as a (Pentagon) operation may not be well received by countries traditionally sensitive to foreign military presence." Islamic extremists have waged insurgencies against countries such as Mali in northern Africa and are suspected in the attack that killed the U.S. ambassador to Libya in Benghazi last fall and three other Americans.

While the Pentagon has taken some steps to coordinate the websites with State Department, senior embassy officials told the GAO the "websites have the potential to unintentionally skew U.S. policy positions or be out of step with other government efforts in a particular country."

The report also pointed out that its reserve forces may not be adequately trained or equipped. In 2006, the Pentagon separated the MISO force into 2,800 special forces soldiers and 4,200 reservists but funded only the active-duty component. The Army's reserve command does not provide funding for language and cultural understanding courses its soldiers are required to have. There is also no dedicated fund to pay for reservists' equipment.

One result, according to the report, is that one reserve company reported asking "local businesses in Iraq and Afghanistan to print MISO products because they did not have working printers, and that these scenarios were not ideal because due to the sensitive nature of the products."

Table of Contents

¡Dios Mío! Pentagon's Latest Weapon in Colombian Drug War? Soap Operas

By Robert Beckhusen, Wired, 05.29.13

The U.S. Army is introducing a new weapon in its fight to get Colombia's guerrillas to put down their guns: the soap opera.

That's the gist of a recent Army request for proposals, which describes the building blocks of an anti-guerrilla propaganda campaign in Colombia. According to the request, the Army wants a potential contractor to write and produce a total of 20 radio novela episodes for an Army MISO team (Military Information Support Operations) based in Colombia, with eight episodes that "convey messages that promote demobilization," or encouraging armed groups to put down their weapons. Another eight "shall convey messages that counter recruitment of target audiences (TAs) into illegal armed groups."

The scripts, according to the request, will be true to life in a way, as they're "derived from statements received by demobilized guerrillas." Final approval before airing will also be reserved by the MISO team, which can demand rewrites. After the 16-episode run, another four episodes will focus on promoting "traditional family values, belief in the respectful treatment of women, democratic alternatives to violence that can furnish functioning state institutions, and emerging environmental concerns in support of U.S. and partner nation goals in Colombia, South America."

The episodes will be in Spanish and a mix of regional Colombian dialects. There will be recurring characters, of course. And each episode will be about 12 minutes long, with an extra three minutes for recaps and previews to "increase TA's interest in the future episode." Pro-tip: the part about "functioning state institutions" should be kept subtle lest you bore the audience.

"FARC commanders spend a lot of time telling foot soldiers that they will be killed, hurt or imprisoned if they demobilize," explains Ana Patel of the Outward Bound Center for Peacebuildng, a former expert on

disarmament with the International Center for Transitional Justice. “For the past couple of years, government officials have asked demobilizing combatants to call their friends who are still in the mountains and tell them that it is safe to demobilize, with a lot of success.” This would have wider reach — owing to the reliance on radio to communicate in rural Colombia.

There’s also no estimate on how much the Pentagon is spending on its Colombian propaganda. But the military’s MISO teams spent $54 million in total around the world in 2012, according to USA Today. Largely, this money — which has reached up to $580 million over years of fighting in Iraq and Afghanistan — goes to pay for 2,800 special forces operatives and 4,000 reservists to produce leaflets and broadcasts that promote the U.S. military and diss insurgents; collect insurgent propaganda; and develop more propaganda in response.

But according to the newspaper, which obtained a critical report about MISO activities from the Congressional investigators at the Government Accountability Office, it’s far from clear whether the propaganda plans are actually panning out. Neither the Pentagon or Congress has “a complete picture” of where the money is going. The programs also lack end goals and no one can measure how well they’re working. Worse, “if used ineffectively, MISO activities have the potential to undermine the credibility of the United States and threaten (Pentagon) and other agencies’ efforts to accomplish key foreign policy goals,” the report noted.

The Pentagon seems to partly agree with the criticisms. Spokesman Lt. Col. James Gregory said in a statement that the Defense Department is “revising both its tracking and reporting requirements” so that regional military commanders “can more accurately and completely account for and report their MISO activities.” Funding for a pilot program is also “being expanded to more comprehensively assess these activities,” Gregory said.

A radio drama that teaches people to stay away from criminal groups might sound innovative, but narco-themed programming is mas viejo in places like Colombia. Spanish-language networks have scored primetime hits throughout Latin America and the U.S. with schlocky — and big budget — cartel dramas, or “narco novelas” like Queen of the South (seen above), El Cartel II, and Without Tits There Is No Paradise. Largely made in Colombia, these are also often set to narcocorrido folk ballads glorifying the gangsters, while also taking criticism for being violence-obsessed and misogynistic.

Because they are. And that’s a problem. The other problem is that it’s likely going to take more than a brief radio drama to counteract that. Still, another idea could be teaching people that it’s okay to welcome former cocaine-slinging guerrillas back into their communities, instead of treating them like outcasts. “Giving people a context for why and how these young people have become part of illegal armed groups may lead to greater acceptance by these communities,” Patel says. “The more these issues of demobilization and reintegration are talked about publicly, the better.”

Table of Contents

Tracking cyberterrorists

By Arnaud De Borchgrave, UPI, May 29, 2013

WASHINGTON, May 29 (UPI) -- Tracking, finding and killing Osama bin Laden required unusual skill, intelligence and courage. Tracking al-Qaida's financial conduits through cyberspace is infinitely more difficult.

Network forensics is one of the world's most challenging assignments -- explained in vivid, dramatic detail by Juan C. Zarate, a former super sleuth in the U.S. government's long campaign to find and disrupt al-Qaida's terrorist funding in the Worldwide Web.

A former assistant secretary of the Treasury and deputy assistant to the president and deputy national security adviser, Zarate's "Treasury's War" is a griping electronic whodunit in a constantly changing environment where inequalities are widening and where technology is destroying more jobs than it creates.

Terrorists and organized criminals use cyberspace speed, secrecy and anonymity in a borderless electronic universe where everything moves at the speed of light -- from self-radicalization and fraud to cyber weapons training and illicit financing.

Al-Qaida and its Associated Movements around the world raise money online where cyberfraud is a global criminal enterprise.

They manage criminal syndicates that acquire thousands of credit cards, withdraw small amounts from each one, ranging from $10-$50, then return them as if they had never been stolen.

The victims invariably keep quiet, only too happy to get their electronic credit cards back on line. Millions of customers don't even notice the loss.

A recent demonstration moved 100 terabits per second through ether-space. Detecting who's doing what to whom at such speeds and then redirecting traffic to foil cyberterrorists is the challenge that cyber sleuths face round the clock, 365 days a year.

Zarate, a senior adviser at the Center for Strategic and International Studies, is a chief architect of modern financial warfare for the U.S. government.

His "Treasury's War" takes the reader into the shadowy world where banks and U.S. Treasury tools come together to foil terrorists and to influence geopolitical outcomes.

From his Treasury and White House offices, Zarate, with a dedicated group of Treasury officials, designed and then led a secret financial war against America's enemies.

This is the first book that lifts the veil of secrecy on the financial power they marshaled against America's enemies.

The financial and cyber warriors, says Zarate, "created an international financial environment in which the private sector's bottom line dovetailed directly with U.S. national security interests -- with the goal of isolating rogues from the legitimate financial system."

The global terrorist funding and illicit financial networks range from the slaughter of elephants (tusks go for $50,000 and up) and rhinoceros (a single horn fetches up to $30,000) in Africa to the heroin trade in Afghanistan.

The United States and its closest allies are also engaged in a new kind of electronic warfare against the financial networks of rogue regimes -- everything from nuclear proliferators to criminal syndicates and their links with transnational terrorist networks.

Zarate takes the reader behind the scenes to explain how the group he led redefined the U.S. Treasury's role, "and used its unique powers, relationships and reputation to apply financial pressure against America's enemies."

The goal was -- and is now 24/7 -- to isolate rogues from the legitimate international financial system. And in so doing, created "a new brand of financial power (that) leveraged the private sector and created an international financial environment in which the private sector's bottom line dovetailed directly with U.S. national security interests."

Treasury and its new tools, Zarate explains in "Treasury's War," soon became critical in all the "central geopolitical challenges facing the United States, including terrorism, nuclear proliferation, and regimes in North Korea, Iran, Syria, Lebanon, Iraq and Cuba."

In addition to CSIS, Zarate is senior national security analyst for CBS News and is a visiting lecturer of law at the Harvard Law School. He was the first assistant secretary of the Treasury for terrorist financing and financial crimes.

Zarate then moved to the White House (under George W. Bush) where he served as deputy assistant to the president and deputy national security adviser for combating terrorism and contraband finance.

He is one of very few speakers who can address immensely complex issues of high-level strategic concern coupled with the intricacies of the financial methods of fighting terrorism.

Zarate is still using the skills he took to the White House -- for the private sector as a consultant.

There is still one critically important part of the electronic puzzle that eludes the combined forces of the electronic Kojak/Columbo/Poirot/Scarpetta/Holmes network. It's the informal, handshake ways of moving money, including Hawala. And Hawala's origins are found in texts of Islamic law that date to the eighth century.

In more recent times, Hawala is a round-the-clock system from scores of pay phones or mobiles in Pakistan, Yemen or any Persian Gulf country at predetermined times to say, for example, "Uncle Jack will airfreight your new suit Friday." Translation: The man who introduces himself as Uncle Jack is good to go with $10,000"

Similar amounts will be conveyed anonymously from these same countries to U.S. numbers. By the end of the year, the amounts usually balance out. If not, the discrepancy is carried over to the next year.

It's money transfer without money movement by word of mouth from one cellphone to another thousands of miles away. Mutual trust is the key ingredient.

After more than a decade of counter-terrorist and anti-money laundering efforts, it is clear that the Hawala code of secrecy survives countless attempts to dismantle it.

The U.S. government tried to regulate and infiltrate Hawala through hawaladars, the bearded ones who sit cross legged on a small rug behind a wooden stand in a dusty unpaved street.

In Quetta, the capital of Baluchistan in Pakistan, friends escorted this reporter to a long line of Hawala stalls. In one of them, different currencies, including dollars, stood in neat stacks next to the hawaladar's baggy pants. Armed guards stood on either side.

Hawala honor system transactions move a lot faster than cashing a check in a Pakistani bank. The old and new methods of moving money may be converging, making the challenge of countering terrorist and illicit finance all the more challenging in the 21st century.

Table of Contents

US Ill-Prepared For EMP Attack

By F. Michael Maloof, WND, 29 May 2013

WASHINGTON – Gen. Robert Kehler, commander of U.S. Strategic Command, which oversees U.S. ballistic missile and strategic bombers, has just dropped a bombshell by stating his forces may not be fully prepared for an electromagnetic pulse attack from an adversary capable of launching a nuclear weapon aimed at the United States, according to a report in Joseph Farah's G2 Bulletin.

"I am concerned about the threat of electromagnetic pulse," the STRATCOM chief recently told the Senate Armed Service Committee. "There are some pretty good books that have been written here recently about this, a couple of novels that were written that – that you turn a page looking for the happy ending and it never comes in the book.

"And so I would tell you that we are still mindful of electromagnetic pulse. It is not a Cold War relic," Kehler warned. "It is something that we need to prepare some of our systems to deal with in the operational environment.

"We have a lot of work to do," he cautioned. "I am not yet comfortable that we have gone anywhere near where the magnitude of this problem should take us."

The issue arose in connection with Congress getting assurances on the survivability of STRATCOM's mission.

"We should expect the Defense Department to protect its equities from EMP, and independent expert reviewers should carefully scrub its work, as was done during the Cold War," said former Ambassador Henry Cooper, the first director of the Strategic Defense Initiative under President Ronald Reagan.

While it is imperative for the Department of Defense, or DOD, to ensure its equities are protected in the case of an EMP event, Cooper said that it isn't up to DOD to ensure the viability of the nation's critical infrastructures, particularly its vulnerable electrical grid system and all those that rely on electronic components and automated control systems.

"Logically, one would assume the Department of Homeland Security should provide integrated guidance and a government-wide integrated approach to assuring the viability of all critical infrastructures under all stressful conditions," Cooper said. "But DHS does not even include an appropriate scenario to encourage various government agencies to deal with EMP effects."

What Cooper was referring to are the 15 National Planning Scenarios that DHS has developed on what action to take in the event of a national catastrophe, such as natural disasters or terrorist attacks. However, DHS has not devised a NPS for an EMP event, whether natural or manmade.

The National Aerospace and Space Administration also has warned that the nation and indeed the planet could sustain a direct hit from some of the X-class solar flares that increasingly are spewing off of the sun's surface.

If that happened, NASA projects that because of the vulnerability of the national electrical grid and critical infrastructures that rely on electronic components and automated control systems, this nation alone could sustain damages amounting to some $2 trillion, take anywhere from four to 10 years to recover, if ever, and affect the lives of some 160 million people, meaning death and starvation.

He said that the Department of Energy could lead in assuring the electric power grid will survive an EMP event "but hasn't yet made much progress in doing so," he said.

Table of Contents

Waging the Cyber War in Syria

By Ronald Deibert, Special to National Post, 21 May 2013

Another day, another hacker exploit. Only this time the perpetrator was not Anonymous or LulzSec or any of their hacker sympathizers. In February 2012, a group called the Syrian Electronic Army (SEA) posted on Internet forums the email credentials, including usernames and passwords, of Al Jazeera journalists, as well

as a series of emails purporting to show bias in their coverage of the Assad regime. We learned about this breach the same way most other concerned observers did: when the SEA boasted about it on their Arabic Facebook page. Assad's cyber warriors have set up hundreds of them. Whenever Facebook administrators delete the page — for inciting violence or using Facebook to disseminate links to malicious software — the SEA simply creates a new page with a new domain name. It's an online version of Whac-A-Mole, only in this case it's not a game. It's war.

The SEA also has a Twitter account, through which posts are made in Arabic that taunt its adversaries or boast about its latest exploit. For example, on July 5, 2012, the SEA managed to take over the Twitter account of Al Jazeera's The Stream — possibly acquiring the sign-up credentials through a previous computer breach of Al Jazeera's servers — and then took credit for the hack on its Twitter account, @Official_sea. For a few hours on that July day, to the bemusement of many Twitterati, they used Al Jazeera's account to turn the broadcaster's coverage upside down: from an independent monitor of atrocities to a mouthpiece for the Assad regime.

The Citizen Lab, a Toronto-based group that monitors the use of cyberspace for political purposes, turned its attention to the SEA when the Arab Spring blew into the streets of Damascus in early 2011. Amidst the smoke and rubble of an increasingly violent civil war — and after the UN monitors finally reported that "crimes against humanity" were being committed by the Syrian regime — another type of warfare took shape, this one through radio waves and fibre-optic cables, and over social media platforms.

Like the Tunisians, Egyptians, and Libyans, angry Syrians opposed to the dictatorial ways of their government and looking to ignite a revolution reached instinctively for the latest tools of the digital age. The anti-Assad "Day of Rage," announced to the world through Arabic Facebook, Twitter, and on other social media platforms in February 2011, set the tone. The Syrian protesters built on lessons learned from other digitally empowered protests, and benefited from a growing grassroots movement of technological peer support. Hacktivist groups like Telecomix and Anonymous jumped into the fray by breaking into Syrian government computers, distributing secure tools to circumvent Internet censorship, and helping expose companies that provide services to the Assad regime. In February 2012, Anonymous broke into the email server of the Syrian Ministry of Presidential Affairs and published hundreds of emails.

Neighbouring states and great powers meddled, too. While Russia and China stymied UN resolutions to sanction Syria, Iran's Revolutionary Guard's elite signals intelligence unit roamed Syrian city streets in black vans and employed sophisticated surveillance tools to triangulate the location of dissidents using insecure satellite phones. On the other side of the battle, American and British officials provided tools and training for the armed opposition in the Free Syrian Army, while the Canadian government quietly used its diplomatic headquarters in Ankara, Turkey, to channel information to those fighting the Assad regime.

As a result of such outside support, those opposed to Assad are technologically well equipped. The latest generation mobile phones have been employed as frontline sensors, uploading atrocities for the world to witness as they occur, thus circumventing the Syrian regime's official blackout of journalists. The Citizen Lab's senior Middle East and North Africa—based researcher, Helmi Noman, has shared many of these videos with our Toronto staff, translating the horrific scenes from Arabic to English so that we could understand that protesters were being buried alive at gunpoint, forced to swear allegiance to Assad while they drew their last breath; that tidy lines of corpses covered in blood-stained white sheets, some clearly children, were the victims of deliberate Syrian military attacks on the country's own people in its own cities.

But the familiar script of digitally enabled pro-democracy activists outflanking flat-footed tyrants, which played itself out in other theatres of the Arab Spring, never fully materialized in Syria. The Assad regime adapted and evolved, taking its counter-insurgency tactics to the virtual plane. After various ham-fisted attempts at control, Syria decided instead to actually loosen its grip on cyberspace.

By loosening controls over particular Internet platforms — especially those used by protesters to organize — the Syrian regime acquired unparalleled insights into its adversaries' thoughts, plans, and actions.

The regime took an ever greater step into the market for surveillance.

As the conflict unfolded, reports began to surface about a dark market in high-tech equipment — the products and services coming mostly from Western firms — used by the regime. In a series of investigative reports, Bloomberg News revealed that an Italian company, Area SpA, was installing a surveillance system that would enable the Assad regime to intercept, scan, and catalogue emails flowing through the country. The report was the tip of an iceberg.

The Citizen Lab helped uncover that routers belonging to Blue Coat Systems, an American company based in Sunnyvale, California, were widely deployed across the Internet in Syria. The Blue Coat devices could be used to filter content and monitor communications in fine-grained detail. Under U.S. sanctions against the sale of

products and services to Syria — designated a “state sponsor of terror” by the American government — any business relationship between Blue Coat and Syria was illegal. The European hacker collective Telecomix was on the same trail as the Citizen Lab, and we both published our findings in November of 2011.

We found that the website of Al-Manar, the media wing of the Lebanese militant group Hezbollah, was hosted on the same Montreal-based servers — in violation of Canadian sanctions.

It created a firestorm, including calls for a U.S. Congressional investigation into Blue Coat. The company later acknowledged the presence of their devices in Syria, but said they were shipped to the country fraudulently and without their knowledge, a dubious claim. As Blue Coat’s primary function is to monitor Internet traffic, and their devices only function properly when checking in to get updates from central Blue Coat servers, such a claim was too far-fetched to be credible. These and other revelations of high-tech surveillance equipment being imported into Syria underscored the other side of a regime that once attempted to control the Internet through censorship: targeted surveillance is far more effective.

Just as the Citizen Lab was preparing its Blue Coat report, we stumbled upon a number of Syrian government websites that were hosted on Canadian servers, including the state-backed television station, Addounia TV, that had been placed on an official sanctions list by Canada and the European Union for incitement of violence. The content being streamed online by Addounia TV claimed that the atrocities captured on film by Syrian protesters were fabrications, and it encouraged Syrians who supported Assad to take to the streets and fight back. We also found that the website of Al-Manar, the media wing of the Lebanese militant group Hezbollah, was hosted on the same Montreal-based servers, again in violation of Canadian sanctions. Reflecting on the role media have played in inciting genocide in places like Rwanda, we decided to publish our findings immediately. Called The Canadian Connection: An Investigation of Syrian Government and Hezbollah Web Hosting in Canada, our report no doubt caused a few red faces in Foreign Affairs and International Trade Canada, but it also underscored the complexity and difficulty of imposing effective international sanctions over cyberspace activities.

High-tech surveillance equipment in Syria and Syrian government web hosting in Canada were only part of the story of Syria’s metamorphosis from an Internet-phobic regime to one that embraces technology in the service of armed struggle and civil repression. The SEA’s first forays into cyber war were amateurish — it defaced websites, the online equivalent of graffiti; spammed the comments sections of online forums and newspapers, the actions of a pest more than a menacing army; and targeted websites and forums that appeared to have no relation whatsoever to Syria (the website of an obscure town council in Britain, Harvard University, and so forth), juvenile acts of opportunism. Anyone with a few hours to spare can easily Google instructions and then scan the Internet looking for poorly patched servers waiting to be plucked and desecrated.

But over time, and especially into 2012, SEA evolved.

In the spring of 2012, the Electronic Frontier Foundation started receiving reports from inside Syria of attacks on Facebook, YouTube and other social media outlets used by Syrian dissidents. When users clicked on links posted on the comment sections of opposition sites, they were taken to fake websites that encouraged them to download special software, which was then used to acquire their credentials and sometimes to take over their computers. The EFF also discovered an instance of a malicious software program hidden in images circulated among Syrians in the diaspora.

Although EFF could not confirm the identity of the perpetrators, they suspected that the Syrian telecommunications ministry was behind the attacks. Meanwhile, reports of authorities using force against activists and dissident Facebook users, and demanding their login information, surfaced. In one case, a user was beaten by Syrian police, who then informed him that they had been reading his “bad comments” on Facebook. After providing his password to authorities, he was imprisoned for two weeks. Upon his release, he found that somebody had logged into his Facebook account and posted pro-regime comments in his name.

Google computer security analyst Morgan Marquis-Boire and UCLA Ph.D. student John Scott-Railton were involved in the EFF’s work, and in 2012 they contacted the Citizen Lab to suggest combining research efforts with EFF’s Eva Galperin. (Marquis- Boire and Scott-Railton later joined the Citizen Lab as research fellows.) Together, our teams uncovered one targeted attack after another on Syrian dissidents, typically engineered by commandeering someone’s computer and using that person’s Skype or email account to trick the dissident’s network of contacts into clicking on links or opening files that contained malicious programs. These were precision attacks. Our researchers watched as the cyber raids became more persistent and sophisticated, and showed significant knowledge of criminal hacking techniques.

Although we found no smoking gun connecting these attacks directly to the Syrian government, the majority were clearly engineered by individuals connected to command-and-control computers operating on Syrian

telecommunications networks registered in Damascus. The Syrian government was either tacitly condoning or actively encouraging the SEA, a marked turning point in how an autocratic regime deals with a digitally mobilized opposition. Dictators have little to fear from technology: it can be their best friend.

Table of Contents

Globalization Creates a New Worry: Enemy Convergence

By Thom Shanker, New York Times, 30 May 2013

WASHINGTON — Adm. James G. Stavridis, who stepped down this month as NATO's supreme commander, has been at war in two wars — overseeing the alliance's role in the enduring mission in Afghanistan as well as the shorter combat air campaign over Libya.

Combined with his tenure before NATO — he was the top officer at the military's Southern Command, for a total of seven years in a senior four-star billet — Admiral Stavridis had been the longest-serving global combatant commander in the American military.

As he rose through the ranks of command over a 37-year career in uniform, Admiral Stavridis also came to be recognized as one of the military's most prolific authors on strategy, operations and tactics. Today, though, ask what worries him most, and he answers in a single word: convergence.

That is the new term of choice in national security circles for the coming together of previously unrelated adversaries, who not only might combine in operations, but also share resources, know-how, weapons and technology and personnel.

"This is really the dark end of the spectrum of globalization as you assess rising national security risks," Admiral Stavridis said in an interview. "It is something I worry about enormously."

What might convergence look like?

Drug cartels along America's southern border, whose smuggling operations move contraband and people into the United States, might come to make common cause with terrorist or militant organizations to bring in weapons or bomber makers.

"I think that's a very possible and very dangerous business model, and you have to prevent narco-businessmen crossing those streams with the terrorists," Admiral Stavridis said.

"What the narco-confederacies offer are routes, the trafficking capabilities — moving matériel and people," he added. "If you can move 10 tons of cocaine into the U.S. in a small, semi-submersible vessel, how hard do you think it would be to move a weapon of mass destruction?"

Although it had long been assumed that drug traffickers would not want to adopt political or militant activities for fear of bringing down even harsher American might to suppress their for-profit operations, Admiral Stavridis said that "for the right level of inducement — for the right amount of money — it could happen."

He said there were signs already of operatives "with a foot in both camps, including Hezbollah."

For example, American law enforcement officials have said they thwarted an Iranian-backed plot in 2011 to co-opt members of a Mexican drug gang to kill the Saudi ambassador to Washington. And the Taliban underwrite their operations in Afghanistan via the poppy trade.

Admiral Stavridis also sketched a scenario in which a country like North Korea, seeking to attack the United States or its allies without the clear and obvious attribution of a missile launch, might contract with a smuggling ring to move a weapon into a major port somewhere in the world.

Those assessments on future national security risks will be carried by Admiral Stavridis to his next job, in academia, as dean of the Fletcher School of Law and Diplomacy at Tufts University.

Assessing other significant transformations to the modern way of war, Admiral Stavridis underscored the sea change in the amount and movement of information on the battlefield.

"My smartphone has more communications capability, and can manage more information than the $500 million destroyer I first sailed in 1977," he said. "And that's by orders of magnitude."

He gave the military only a "B+" grade for its abilities to leverage the revolution of information, including the emergence of social networks, in reshaping the ways local populations interact among themselves and with their governments.

Also worrisome, he said, is how adversaries show great agility in using information against the United States and its allies. The future of security for the United States is to build up its own physical networks of alliances, coalitions and partnerships, he said.

“The 20th century was all about building walls: The Maginot Line, the Siegfried Line, the Iron Curtain, the Bamboo Curtain and the Berlin Wall — we built walls everywhere,” Admiral Stavridis said. “How did that work for us? Sixty million dead in two world wars, a continent destroyed in Europe and much of Asia destroyed, as well.”

For the 21st century, he said, “We cannot create security with walls. You have to build bridges. It will be all about alliances and coalitions. And the military has to build bridges to the civilian sectors to create security.

“We will still need our guns,” he concluded. “There are times we have to apply lethal force. Soft power alone is like no power. But combining soft and hard power is smart power.”

Table of Contents