THE FEET OF THE MASTERS: LESSONS ON IRREGULAR CYBER WARFARE

Articles

José de Arimatéia da Cruz and Travis Howard

The United States invented the Internet. Andrew Blum's chronicle of the Internet's vast inner workings in *Tubes: A journey to the Center of the Internet*(2012) describes the moments the ARPANET went live on October 29th, 1969, digitally hand-shaking with another university's SDS Sigma 7 host computer in a cramped room on the University of California Los Angeles (UCLA) campus. U.S.'s academic ingenuity and engineering expertise brought life to what is today "cyberspace." The birth of the Internet would launch the world into the Information Age, with the U.S. leading the charge. Cyberspace and the Internet are American inventions, reflecting American values, which are used in all nations by all generations (Healey, 2016: 17). As the world becomes more interconnected and complex, warfare theorists immediately went to work in discovering how the Internet could be harnessed for defense-purposes (it was, after all, started as a project supporting the U.S. Department of Defense). Cyberwarfare becomes a force multiplier in any kinetic conflict between nation-states. As Courtney Weinbaum, a management scientist at the RAND Corporation, and John N.T. Shanahan, retired Air Force Lieutenant General currently the Director for Defense Intelligence (Warfighter Support) in the Office of the Under Secretary of Defense for Intelligence, argue, "the future battlespace is constructed of not only ships, tanks, missiles, and satellites, but also algorithms, networks, and sensor grids...future wars will be fought on civilian and military infrastructures of satellite systems, electric power grids, communications networks, and transportation systems, and within human networks" (Weinbaum and Shanahan, 2016:4).

With such a head-start, why are we losing the cyber war today? Alexander Klimburg, in his 2017 book *The Darkening Web: The War for Cyberspace*, describes how nation states have drastically different views on what "information warfare" means – while the U.S. has been happily using the Internet for what it was intended, sharing ideas and generating wealth, her adversaries were finding ways to exploit it following the timeless art of warfare, but adapted for a digital age. In short, while we were contemplating how cyberspace has changed human interaction, China and Russia, perhaps North Korea and Iran, were contemplating how to use the global reach of the Internet as a new tool for centuries-old warfare practices.

What lessons could strategic warfare masters tell us about 21st century insurgent cyber warfare, where superpowers could be brought low by small cells of cyber warriors with limited funding but lots of time? This article distills the wisdom of two military strategists: Chinese General and 6th century Taoist military philosopher Sun-tzu, and Carl Philipp Gottfried von Clausewitz, Prussian general and theorist of psychological and political aspects of warfare as well as revolutionary thinkers such as Mao Tse-tung,

Carlos Marighella, and Ernesto "Che" Guevara. This article seeks to take the insurgency viewpoint: as an insurgent, which is in a weaker power position vis-a-vis a stronger nation state; how does cyber warfare plays an integral part in the irregular cyber conflicts in the twenty-first century between nation-states and violent non-state actors or insurgencies.

Sun-tzu: Harnessing the Tao of Cyber Warfare

Most modern military officers and scholars familiar, if not well-versed, in the teachings of the ancient Chinese military strategist Sun-tzu: one of the *Seven Military Classics* thought to have been originally compiled in the second century B.C., after over a thousand years of warfare, violence, and conflict in the Far East dynasties. Multiple works have been written and translated over the last two thousand years, interpreting Sun-tzu's texts for increasingly-modern military strategies and technology. While notable work such as Geers' (2011) *Sun Tzu and Cyberwar* have been written to decipher Sun-tzu's teachings for cyber and information warfare, we will focus on how Sun-tzu, as an insurgent force with fewer resources, would wage cyber war against a larger, more powerful nation state (See Table 1).

Table 1. Sun-tzu
Chinese General and 6th century Taoist military philosopher

Lessons for Cyber Insurgents	Lessons for Nation States
- Emphasis on deception, feints, subterfuge; be unpredictable - Sow confusion in social media - Avoid a single prolonged cyber operation, but "play the long game" in generating long-term cyber effects - Turn the enemy's infrastructure against them	- Fight confusion and deception with a clear strategy, concise instructions to fighting force, and - Create contingency plans for loss of command and control functions - Be prepared for cyber effects at all times, know the symptoms - Conduct extensive cyber wargaming

Much of Sun-tzu's writing in his first text, *Initial Estimations*, discusses how unpredictability and paradigm-shifts lead to military victory. The emphasis on deception, feints, subterfuge, and illusions indicate that Sun-tzu would feel comfortable employing all manner of non-kinetic cyber effects if it meant gaining an advantage over his adversaries. In particular, sowing discord among the enemy ranks through propaganda and mass misinformation would be the most favored approaches. Social media, as a platform, excels at doing just that. Additionally, cyberspace is the near-perfect platform to sow confusion among adversaries using a few hacked social media accounts. For example, after the Boston Marathon bombing in April 2013, the Associated Press' Twitter account was hacked by a group identifying itself as the Syrian Electronic Army (SEA). The group released a fake headline titled "Breaking: Two Explosions in the White House and Barack Obama is injured." The SEA's action resulted in a sharp decline in the New York Stock Exchange (NYSE). However, once the news of the explosion was discovered to be false, to the relief of investors, NYSE returned to normalcy (Kan, 2013: 1). The point was made: misinformation can have real effects.

Insurgent groups looking to take advantage of a more powerful nation's computerized critical infrastructure and its reliance on a digital economy can easily see the advantage gained through a more prolonged cyber-deception campaign, especially if they shifted to more subtle, coercive means than an obviously-fake headline. The recent societal fight against "fake news" is an example of such a campaign, potentially waged (at least in part) by nation states opposed to the United States and the allied Western democracies. A drawn-out effort within cyberspace, however, might not be what Sun-tzu would recommend; he cautioned against "protracted warfare" and "prolonged campaigns" (Sun-tzu, 1994: 173). In Sun-tzu's case, he was discussing the logistic challenges involved in supplying an army for a long duration, and perhaps domestic challenges associated with "war fatigue," a challenge that the United States knows too well. In cyberspace, however, a prolonged campaign by covert insurgents, in which non-attribution is key, can prove hazardous as the targeted nation's cyber defense adapts and maneuvers to respond. For a less powerful insurgent group, this could mean the stronger, bigger nation could respond with kinetic, traditional military force.

Sun-tzu's idea of irregular warfare advocates for converting the enemy's resources, such as manpower, equipment and supplies, rather that destroying them; this is what he describes as "conquering the enemy and growing stronger" (Sun-tzu, 1994: 174). Geers noted that Sun-tzu's recommendation could have positive effects on warfare as a whole, with fewer physical casualties and positioned for access post-war recovery and diplomacy (Geers, 2011: 6). This does not make cyber-effects any more devastating to the target nation's citizenry, however, since in the 21st century most major powers' economies and critical infrastructure rely almost exclusively on digital information; a cyber attack would constitute an act of war and cause major disruption to the nation.

Perhaps Sun-tzu's strongest approval for information and cyber warfare as a sound insurgency strategy can be found in his third text, *Planning Offensives*, in which he proclaims that "the highest realization of warfare is to attack the enemy's plans; next is to attack their alliances" (Sun-tzu, 1994: 177). In this instance, an established and more powerful nation state, conforming to conventional warfare strategy and laws, is at a disadvantage against a more agile cyber-insurgent force. Today's Sun-tzu would be apt to use cyber-effects to disrupt planning tools and the common operational picture (COP); he would use cyber warfare problematic attribution to sow seeds of confusion and misinformation amongst allied nations and coalition forces thus creating a "fog of war." The penchant for hacking groups (state sponsored or otherwise) to leak privileged or classified information to undermine alliances and tarnish reputations is a key example of such a tactic.

Sun-tzu would ultimately use cyber-insurgency to "play the long game" using cyber-effects to diminish a more powerful nation state's economic and political power on the world stage. He would do this through carefully-planned attacks on the information assurance of military planning and COP tools, rendering their use unreliable and their data suspect. He would steal sensitive intelligence and make politically-damaging information public at strategic times, fanning the flames of civil discourse and economic down-turn with sensationalized "fake news" stories that cause mass confusion and outrage. The latter effects would also demoralize the enemy's military and sour the citizenry towards the commitment of physical military force for any extended duration. Ultimately, in a 21st century global economy powered by information technology, what Sun-tzu would consider the "strategic configuration of power" would most certainly involve mastery of cyberspace and the tenants of irregular, insurgent-style information warfare (Whitham, 2012).

How can a large nation-state, with vast resources but unwieldy policy and financial controls, apply the lessons of Sun-tzu to irregular cyber-warfare? There are several key themes from Sun-tzu's writing that, when applied to 21stcentury irregular cyber-warfare, allows one to make several observations. First, fight confusion and deception with clear strategic vision, concise orders, and an uncomplicated and unified chain of command. Second, fighting irregular warfare requires an irregular battle plan: our forces must be agile and unpredictable, and we must manipulate the battle space in our favor. Third, if in a prolonged campaign, be prepared for insurgent cyber effects, and expect them to be more devastating and desperate the longer the campaign progresses. Finally, conduct extensive wargame-like exercises with a red team (voice of the adversary), and always "give the enemy a vote" in your planning.

Carl von Clausewitz and Cyber Insurgency: Absolute or Limited Cyber-Warfare to Achieve Political Goals

To contextualize the work of the Prussian General Carl von Clausewitz in the modern era of cyber-warfare, it is important to understand the historical context within which he based his ideas. Michael Howard and Peter Paret translation of Clausewitz's *On War* offers essays that give us some context: "The most important task that faced Prussian soldiers in the opening years of the nineteenth century was to come to terms intellectually and institutionally with the new French way of warfare" (Clausewitz, 1976: 9). Thus, in von Clausewitz's time, Napoleonic strategic and military tactics were largely seen as radical, fluid, and (quite literally) revolutionary, in much the same way cyber warfare is being employed today (See Table 2).

Table 2. Carl Philipp Gottfried von Clausewitz
Prussian General and 19th century military theorist

Lessons for Cyber Insurgents	Lessons for Nation States
- Treat cyberspace as a warfighting domain to achieve rapid effects in a limited war - Fight asymmetrically, conduct cyber-attacks to create non-cyber physical results - Use cyber warfare as a means to achieve political and strategic objectives	- Treat cyberspace as a warfighting domain and resource appropriate offensive and defensive power - Warfare is constantly changing, doctrine must be adaptable or, in some cases, completely rebuilt - Never stop innovating

One might be forgiven for mistaking von Clausewitz as a more "traditional" military strategist and intellectual with a good portion of his work describing the "nuts and bolts" of military matters such as logistics, command and control, rules, regulations, and routines. Deeper study reveals him instead to have an understanding of the ever-changing, accelerated nature of warfare. In fact, the Prussian General came to understand that "there was no single standard of excellence in war" nor could strategy be broken down into a universal formula; warfare was nebulous, it was unpredictable, and "dead theories" could not be relied upon to win the day (Clausewitz, 1976).

Clausewitz's work, although unfinished before his death, centered around two themes when analyzed with his other writings and notes. First, the "dual nature of war, as an instrument which could be used either to overthrow the enemy [absolute war] or two exact from him a limited concession [limited war]." Second, "war is simply the continuation of policy by other means" (Clausewitz, 1976: 28). Clausewitz, as a cyber-insurgent, would have likely used cyber-attacks to great effect in a limited war, possibly as one of the primary elements in a campaign to undermine political interests of the targeted state. Lacking true military strength to fight asymmetrically in traditional, kinetic warfare roles, conducting cyber-attacks to achieve kinetic effects could be a favored Clausewitz strategy. An example of achieving kinetic effects through cyberspace includes targeting Industrial Control Systems (ICS) to damage moving machinery within an infrastructure, otherwise known as SCADA attacks. Such attacks have been proven to damage centrifuges, turbine engines, and other fast-moving machines by sending improper control signals.

Clausewitz's view of an absolute war would involve all elements of warfare. In a war, from the perspective of a lesser power against a greater power, he would certainly take advantage of ICS/SCADA cyber-attacks in order to damage an enemy's critical infrastructure and force them into an unfavorable strategic position. Damaging the enemy's civilian and governmental infrastructure limits its ability to make war, and for Western countries with democratic and open society these attacks can pressurize political bodies to find ways to end the conflict. This seems to satisfy both of Clausewitz's tenants regarding the dual nature and political characteristics of war.

Consider this scenario: a U.S. Carrier Strike Group makes way northbound through the Red Sea, having just passed through the Gulf of Aden and Bab-el-Mandab Strait. The guided missile destroyer escorts shield the capital ship from small craft off of the coast of Yemen, using intelligence, surveillance, and reconnaissance (ISR) assets to identify and track surface targets. Suddenly, jammers in a few of the small boats within a fishing group go active, creating a localized electromagnetic jamming field that partially blocks satellite communications and disrupts global positioning signals. Simultaneously, malicious code successfully planted within the combat systems of two of the surface combatant escorts releases its payload, causing disruptions and latency that slow the threat response times of those units' combat information centers. Thirty seconds later, a stream raid of C802 anti-ship cruise missiles (ASCM) are fired from truck-mounted coastal batteries along the Yemeni coast, saturating the battlespace with six missiles simultaneously.

While the combat systems suites aboard the modern naval combatants are more than a match for older, outdated anti-ship cruise missiles, a simultaneous cyber-attack and ASCM stream-raid against those combat systems can disrupt self-defense actions. Of course, this is a hypothetical scenario and is presented without many details and certainly with many assumptions; however, it serves to illustrate how a weaker power

could use a cyber-attack combined with low-cost and prolific kinetic weapons to target a more powerful state's center of gravity. Clausewitz would likely be a proponent of such tactics, evoking his very definition of war: "the act of force to compel our enemy to do our will" (p. 75). To wit, Clausewitz explains that military force "equips itself with the inventions of art and science" and that the true aim is to "render the enemy powerless" (Clausewitz, et al., 1976, p.75). The proliferation of information technology and always-connected command and control (C2) makes precursor cyber-attacks a near certainty in 21st century warfare, and of particular interest to cyber-insurgents who have everything to gain but little to lose in relation to its larger adversary.

Like Sun-tzu, we can also find Clausewitz's ideas being applied to cyber defense and strategy. The Prussian General's definition of the "dual nature of war" (absolute war vs. limited war) and his acknowledgement of extreme violence as a victory condition begets an "all-in" approach to counter violent attacks that use cyber-effects as a precursor to kinetic strikes. This requires large nations that are at risk from smaller insurgencies to be prepared to use force if necessary to exterminate the threat decisively. Warfare is ultimately a political means to an end; cyber-war is strictly a military affair, but an affair of the state and can be affected by the proper use of diplomacy and political leverage. Finally, that warfare does not fit a mold or rulebook, but is adaptable and always changing, means that the defending nation cannot stop innovating or investing in research and development related to war, lest the enemy achieve the first breakthrough that will change the dynamic. In no area of warfare is this truer than in the cyber domain, only much, much faster.

Carlos Marighella and the *Minimanual of the Urban Guerrilla*

Carlos Marighella (December 5th, 1911-November 4th, 1969) was a Brazilian Marxist revolutionary and writer. While Marighella's guerrilla rendezvous occurred prior to urban guerrilla use of the Internet, nonetheless his views on the use of the means of public communication are as relevant today as they were in the 1960s at the zenith of Marighella's guerrilla activities (See Table 3). In fact, the *Minimanual of the Urban Guerrilla* published in June 1969 by the Ação Libertadora Nacional (National Liberation Action, ALN) defends the use of the means of public communication to demoralize the legitimate government in power. As Bruno Paes Manso and Camila Nunes Dias report, in August 15, 1969, twelve guerrilla fighters associated with the ALN invaded the radio station, Rádio Nacional, to transmit a statement on behalf of Marighella against the Brazilian dictatorship which came to power in 1964 and in favor of a popular government (Manso and Dias, 2018, 145). In 1920, T.E. Lawrence stated that, "the printing press is the greatest weapon in the armory of the modern command" (*Counterinsurgency Field Manual*, 2007: 7). In the twenty first century interconnected and globalized world, with the development of new technologies and the Internet, violent non-state actors, terrorist groups, criminal organizations "using the Internet, insurgents can now link virtually with allied groups throughout a state, a region, and even the entire world" (*Counterinsurgency Field Manual*, 2007: 8). As Marighella once point out, "the accusation of violence or terrorism no longer has the negative meaning it used to have...Today, to be violent or a terrorist is a quality that ennobles any honorable person, because it is an act worthy of a revolutionary engaged in armed struggle against the shameful military dictatorship and its atrocities" (Marighella, 2011: 8). The duty of a revolutionary is to make revolution by any means necessary.

Table 3. Carlos Marighella

Marxist Brazilian and 20th century guerilla warfare leader and politician

Lessons for Cyber Insurgents	Lessons for Nation States
- Use cyberspace as a command and control mechanism to connect disparate fighting forces - All insurgent fighters must understand cyberspace as a tool of their trade - Use cyberspace to control the narrative - Spread misinformation to the enemy and mobilize the followers of your cause	- Insurgency command and control methods must be disrupted to prevent coordination - Operational planners must incorporate counter-cyber operations - Combat misinformation with clear public messaging

Marighella, in his essay entitled "*Technical Preparation of the Urban Guerrilla*," argues that "no one can become an urban guerrilla without paying special attention to technical preparation" (Marighella, 2011: 17). For Marighella, the revolutionary should be an expert on anything and everything under the sun in order to advance the revolutionary cause. According to him, a revolutionary should be able to "drive a car, pilot a airplane, handle a motor boat and a sailboat, understand mechanics, radio, telephone, electricity, and have some knowledge of electronics techniques" (Marighella, 2011: 17). Marighella's revolutionaries in today's interconnected technological world would have to have the expertise in ransomware, cryptographic, man-in-the-middle attacks, steganography, and, perhaps most importantly, social engineering. Marighella would probably emphasize today the importance of social engineering which is "essentially the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques" (Hume and Goodchild, 2017). Once in possession of critical and sensitive information obtained via social engineering Marighella's revolutionaries today would disseminate false information in order to undermine the government's legitimacy. As the U.S. Army and Marine Corps Field Manual states, "insurgents take advantage of existing and public media companies through press releases and interviews. These efforts, in addition to using the Internet, broadcast insurgent messages worldwide" (Counterinsurgency Field Manual, 2007: 107).

For Marighella, information represents extraordinary potential in the hands of the urban guerrilla. Marighella endorses the view that the urban guerrilla must "never fail to install a clandestine press and must be able to turn out mimeographed copies using alcohol or electric plates and other duplicating apparatus, expropriating what he cannot buy in order to produce small clandestine newspapers, pamphlets, flyers and stamps for propaganda and agitation against the dictatorship" (Marighella, 2011: 79). Marighella's urban guerrillas today would use spam techniques, Denial of Service (DoS), Distributed Denial of Service (DDoS), the full spectrum of phishing-type attacks, Structured Query Language (SQL) which is a language designed to manipulate and manage data in a database, malware attacks, brute force and dictionary access control attacks just to mention a few of the techniques that would be available. Information in the hands of the urban guerrilla would allow the guerrilla to spread misinformation and mobilize the masses into political protests. Misinformation and political mobilization would lead to the "urban guerrilla demonstrator" (Marighella, 2011: 62).

Ernesto "Che" Guevara and Guerrilla Warfare

Ernesto "Che" Guevara was an Argentine Marxist revolutionary, physician, author, guerrilla leader, and military theorist in the Cuban revolution alongside Fidel Castro. According to I.F. Stone, a reporter who interviewed "Che" during the aftermath of the Cuban revolution, "Che" Guevara had "curly reddish beard, he looked like a cross between a faun and a Sunday-school print of Jesus. Mischief, zest, compassion and a sense of mission flashed across his features" (Stone, pg. viii). "Che" Guevara was a charismatic leader par excellence. The *Counterinsurgency Field Manual* defines a charismatic leader who develop allegiance among their followers because of their unique, individual charismatic appeal, whether ideological, religious, or social" (*Counterinsurgency Field Manual,* pg. 97). Reading "Che" Guevara's*Guerrilla Warfare* and attempting to place it within the context of irregular cyberwarfare obviously is an overstretch. However, "Che" Guevara's discussions of lines of communication, propaganda, and indoctrination would be heavily influenced by the development of the Internet. The Internet would be a force multiplier in its advancement of a revolutionary cause in the twenty-first century (See Table 4.). As a strategy, "Che" Guevara would recognize the maximizing utility of incorporating electronic warfare into irregular warfare. As he states in *Guerrilla Warfare,* "strategy is understood as the analysis of the objectives to be achieved in the light of the total military situation and the overall ways of reaching these objectives" (Guevara, 2012: 8).

Table 4. Ernesto "Che" Guevara

Argentine Marxist revolutionary and 20th century guerilla warfare leader

Lessons for Cyber Insurgents	Lessons for Nation States
- Use electronic means of warfare whenever possible - Use cyber effects to disrupt enemy lines of communication - Use cyberspace to spread propaganda, including lies and deceitful messaging, to create a cultural narrative for action	- Protect critical command and control nodes that have connectivity through cyberspace, including wireless signals - Counter deceitful propaganda with robust public communications campaign to prevent the population from being turned against allied forces

"Che" Guevara, as a revolutionary strategist, pays close attention to the enemy's lines of communication. As he argued, "...surprise attack along the lines of communication of the enemy yields notable dividends" (Guevara, 2012: 18). "Che" Guevara distinguishes between internal and external lines of communication. According to him, "the lines of communication with the exterior should include a series of intermediate points manned by people of complete reliability...the internal lines of communication can also be created. Their extension will be determined by the stage of development reached by the guerrilla band" (Guevara, 2012: 23). Both sources of communication are important for the advancement of the revolutionary ideals but extremely dangerous on the enemy's hand therefore sabotage should be aimed primarily against the enemy's communication apparatus. Therefore, "Che" Guevara advocates that "sabotage on a national scale should be aimed principally at destroying communications. Each type of communication can be destroyed in a different way; all of them are vulnerable" (Guevara, 2012: 94). The importance of the enemy's line of communication is of paramount concern for "Che" Guevara. The line of communications is the blood supplier to the enemy's mission, strategy, and tactics. Destruction of it becomes an important revolutionary goal. As "Che" Guevara points out, "the great strength of the enemy army against the rebels in the flatter zones is rapid communication; we must, then, constantly undermine the strength by knocking out railroad bridges, culverts, electric lights, telephones; also aqueducts and in general everything that is necessary for a normal and modern life" (Guevara, 2012: 95).

Another important aspect of "Che" Guevara's *Guerrilla Warfare* that would resonate with the urban guerrillas of the age of the Internet is importance of propaganda. As "Che" Guevara acknowledges, "every act of the guerrilla army ought always to be accompanied by the propaganda necessary to explain the reasons for it" (Guevara, 2012: 81). Propaganda is an important tool in the arsenal of the urban guerrilla in the age of the Internet. As David Galula in his*Counterinsurgency Warfare: Theory and Practice* pointed out, "the asymmetrical situation has important effects on propaganda. The insurgent, having no responsibility, is free to use every trick; if necessary, he can lie, cheat, exaggerate. He is not obliged to prove; he is judged by what he promises, not by what he does. Consequently, propaganda is a powerful weapon for him" (Galula, 2006: 9). Propaganda provides context, even if deceptive; but most importantly, it creates a cultural narrative for action. A cultural narrative "is a story recounted in the form of a causality linked set of events that explains an event in a group's history and expresses the values, character, or self-identity of the group" (*Counterinsurgency Field Manual,*2007: 93). "Che" Guevara's guerrilla rebels in the age of the Internet would be experts in the areas of encryption, steganography, and cryptography in order to disseminate their ideology and values by creating a "virtual sanctuaries." Sanctuaries were physical safe havens, but in the age of the Internet, terrorists and guerrilla rebels can mobilize, organize, and recruit from safe havens half-away around the world without fear of being captured or prosecuted. These "virtual sanctuaries can be used to try to make insurgent actions seem acceptable or laudable to internal and external audiences" (*Counterinsurgency Field Manual,* 2007: 29).

Mao Tse-tung and *On Guerrilla Warfare*

Mao Tse-tung's *Yu Chi Chan* or *On Guerrilla Warfare* was published in 1937 and it has been widely distributed and translated into several languages. Mao's ideas on guerrilla warfare were influenced by ancient military philosopher Sun Tzu's *The Art of War.* As Samuel B. Griffith points out, "Sun Tzu wrote that speed, surprise, and deception were the primary essentials of the attack and his succinct advice, "Sheng Tung, Chi Hsi" ("Uproar [in the] East, Strike [in the] West"), is no less valid today than it was when he

wrote it 2,400 years ago" (Griffith, 2007:37). In 1938, Mao Tse-tung wrote that "political power comes out of the barrel of a gun." Today, in a globalized and interconnected world of the twenty-first century, political power also come not just from bullets but also bytes (See Table 5.). Information and media activities, according to the*Counterinsurgency Field Manual (2007),* can be an insurgency or violent non-state actor main effort, with violence used in support. Conflicts in the future will closely resemble a "*mosaic war*." According to Conrad C. Crane in his book *Cassandra in Oz: Counterinsurgency and Future War (2016),* a mosaic war is one in which each piece of the conflict is different from each other. You may be fighting several elements within a country. Mosaic war can be either accidental or intentional. In an accidental mosaic conflict "a patchwork of pieces with one well pacified, next to it another one not so pacified or perhaps even under the effective insurgent's control," whereas an intentional mosaic conflict "is created by necessity when the counterinsurgent concentrates his efforts in a selected area is in itself a great enough source of difficulties without adding to it in the selected area" (Galula, 2006: 60).

Table 5. Mao Tse-tung

Chinese Marxist theorist and 20th century Chinese cultural revolutionary leader

Lessons for Cyber Insurgents	Lessons for Nation States
- Develop a mosaic warfare strategy; multiple, disparate efforts generate larger effects - Military victory generates political power - Leverage criminal enterprises and non-government cyber groups for non-attributable attacks	- Operational commanders must recognize different near-simultaneous cyber-attacks in a theater could be part of a coordinated strategy - Track and be prepared to counter non-state actors who could be delivering state effects through non-attributable means

Mao Tse-tung was also well aware of the importance of propaganda as a force multiplier to advance a guerrilla movement ideology. As he stated, "propaganda materials are very important. Every large guerrilla unit should have a printing press and a mimeograph stone" (Tse-tung, 2007:85). Obviously, the days of printing press and mimeograph stone are long gone; today, information is disseminated worldwide by the click of a mouse. In the globalized world of the twenty-first century, nation-states and violent non-state actors will make use of the power of technology to advance their nefarious activities without fear of retaliation, prosecution, or concerns from geographical boundaries. In the "brave new world," a new criminality is emerging in cyberspace. Mao Tse-tung also discusses the importance of organized program to advance the cause(s) of a guerrilla movement. As he states, "the old men organized themselves into propaganda groups known as silver-haired units" (Tse-tung, 2007: 60). In the interconnected world of the Internet today, the "silver-haired units" would meet on cyberspace regardless of geographical location in a virtual safe-haven. They would organize cyber sit-ins by using Denial-of-Service or Distributed Denial-of-Service attacks against the enemy. They would also organize virtual protests to incite outrageous and mobilize the masses into an "urban guerrilla demonstration" (Marighella, 2011: 62).

Conclusions

There is a common theme amongst all of the strategic masters discussed here: innovative, irregular warfare meets its enemy where it is least prepared to receive its effects. To counter it, the defender must adapt and innovate at a rapid pace, and be prepared to leverage considerable resources to do so (See Table 1-5. provided earlier regarding Lessons on Irregular Cyber Warfare). In today's interconnected and globalized world of the twenty-first century, operational commanders must recognize different near-simultaneous cyber-attacks in a theater could be part of a coordinated strategy. Furthermore, leaders must protect critical command and control nodes that have connectivity through cyberspace, including wireless signals. U.S. Navy Admiral Mike Rogers, who retired as the dual-hatted commander of U.S. Cyber Command (USCYBERCOM) and the Director of the National Security Agency (NSA), in a 2017 congressional cyber-posture hearing, underscored the difficulties in meeting irregular warfare in cyberspace by stating: "I would be the first to admit that [information warfare] is not what our workforce is optimized for… we are certainly not where we need to be" (Bing, 2017, para 2).

Admiral Rogers also argues that the traditional signals intelligence-collecting mission of the NSA and externally-focused offensive and defensive missions of USCYBERCOM do not lend themselves to effectively combating adversarial information operations such as digital propaganda, "fake news," and actions that piggyback off of internal U.S. critical infrastructure. Just as friends reconnect through virtual relationships, the Internet leads to political alliances and enmities extending into cyberspace, thereby adding a new and intriguing dimension to traditional state-craft (da Cruz & Alvarez, 2015: 58). Welcome to the "brave new world" of irregular cyber conflict.

The views expressed in this article are those of the authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, Department of the Navy, Pentagon, or the U.S. Government.

References

Chris Bing (2017). *Cyber Command head: We are not prepared to counter info operations*. Cyberscoop.com: Government. Retrieved fromhttps://www.cyberscoop.com/cyber-command-head-not-prepared-counter-info-operations .

Carl Von Clausewitz *On War*, Michael C. Howard and Peter P. Paret (1984).*On War*. Princeton, N.J: Princeton University Press.

José de Arimatéia da Cruz and Taylor Alvarez (2015). "*Cybersecurity initiatives in the Americas: Implications for U.S. National Security,"* Marine Corps University Journal, Vol. 6, No. 2 (Fall): 45-68

Kenneth Geers (2011). *Sun Tzu and cyber war*. CCD CoE, 1-23. Retrieved Apr 19 2017 from http://mirror.picosecond.org/defcon/defcon20-dvd/Speaker%20Presentations/Geers/DEFCON-20-Kenneth-Geers-Sun-Tzu-and-Cyber-War.pdf .

David Galula (2006) *Counterinsurgency Warfare: Theory and Practice.*Westport, Connecticut.

Ernesto "Che" Guevara (2012). *Guerrilla Warfare.* Lexington, KY: BN Publishing.

George V. Hume and Joan Goodchild, "What is social engineering? How criminals take advantage of human behavior," available athttps://www.csoonline.com/article/2124681/social-engineering/what-is-social-engineering.html . Accessed September 21, 2018.

Paul Rexton Kan (2013). *Cyberwar to Wikiwar: battles for cyberspace*. Army War College Carlisle Barracks, PA. Accessed April 19, 2017 available athttp://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA598606 .

The U.S. Army & Marine Corps Counterinsurgency Field Manual (2007). Chicago: The University of Chicago Press.

Bruno Paes Manso and Camila Nunes Dias (2018). *A Guerra: A Ascensão do PCC e o Mundo do Crime no Brasil (The War: The Rise to Power of the PCC and the World of Crime).* São Paulo, SP: Todavia.

Carlos Marighella (2011) *Minimanual of the Urban Guerrilla.* Lexington, KY: BNPublishing.

Stone, I.F. "The Spirit of Che Guevara," in Guevara, E. C. (2012). *Guerrilla Warfare.* Lexington, KY: BN Publishing.

Sun Tzu (1994). *Art of War* transl. R Sawyer. Boulder, Colorado: Westview Press.

Mao Tse-tung (2017). *On Guerrilla Warfare,* transl. Samuel B. Griffith. Lexington, KY: BN Publishig.

Courtney Weinbaum and John N.T. Shanahan, “Intelligence in a Data-Driven Age,” in *Joint Force Quarterly (JFQ)* Issue 90, 3rd Quarter 2018: 4-9.

Ben Whitham (2012). *Exterminating the Cyber Flea: Irregular Warfare Lessons for Cyber Defense*. Retrieved Apr 19 2017 fromhttp://ro.ecu.edu.au/isw/50/ .

Categories: irregular warfare - cyber warfare

Share this Post

About the Author(s)

Travis Howard

Lieutenant Commander Travis Howard is a U.S. Naval Officer with over 18 years of active duty experience in surface and information warfare, with advanced degrees in Business Administration and Cybersecurity Policy, and is a certified information systems security professional (CISSP). He is a frequent contributing author in several Navy and IT professional journals and online publications.

José de Arimatéia da Cruz

Dr. José de Arimatéia da Cruz is a Professor of International Relations and International Studies at Georgia Southern University, Savannah, GA. He also is an Adjunct Research Professor at the U.S. Army War College, Strategic Studies Institute, Carlisle, PA, and a Research Fellow of the Brazil Research Unit at the Council on Hemispheric Affairs in Washington, DC.