Marines with Bravo Company, 1st Battalion, 7th Marine Regiment, provide outboard security after offloading from CH-53E Super Stallion helicopter during mission in Helmand Province, May 1, 2014 (U.S. Marine Corps/Joseph Scanlan)

Forensic Vulnerability Analysis

Putting the "Art" into the Art of War

By Darryl Williams

The supreme art of war is to subdue the enemy without fighting.

—Sun Tzu, *The Art of War*

Is warfare art or science? The debate, touched upon by Sun Tzu in the 6th century BCE, is still raging today. Most scholarly literature states that war is a combination of both art and science.

Lieutenant Colonel Darryl Williams, USAF (Ret.), is the President and Chief Executive Officer of Partnership Solutions International.

Many military scholars side with the argument that the planning and execution of warfare are art, but the tools used to wage war are science. However, in this technology-centric era of large data collection, asymmetric adversaries that employ emerging technologies, nation-states that leverage technology superior proxies, weapons that evoke a *Star Wars* familiarity, and a generation of warfighters that is more comfortable around instantaneous data flows than long-term incremental research, science is taking a more prominent role in warfare. For example, watch the current Department of Defense (DOD) recruiting videos. Except for the Marine Corps, which is still looking for *The Few, The Proud*, most if not all Service recruiting videos focus on technology (for example, jet fighters, cyber warriors, and space warriors).

In the kinetic arena, as weapons and weapons systems become more complex, planning and execution are moving away from art toward more reliance on science. In conflicts up to and including Vietnam, targeting was a matter of saturation to ensure destruction. However, in Operation *Desert Storm*, the public first witnessed precision-strike capabilities. Few who were in the military in 1991 can forget General Norman Schwarzkopf, USA, walking the press through the use of laser-guided bombs in Iraq, Tomahawk cruise missiles launched from ships in the Red Sea, and air-launched cruise missiles from bombers hundreds of miles from the conflict zone. In current conflicts, the integration of global positioning systems into bombs allows one B-2 to effectively prosecute 80 targets. In future conflicts, emerging directed energy weapons will enable the possibility of surgical attacks with little to no collateral damage. The bottom line is that kinetic warfare is becoming more about the science of the tools than the art of the application.

Even in the nonkinetic arena, warfare is becoming more science than art. It is all about the science behind the tools used. Executing a broad-brush, nonkinetic attack is easy and science-centric. If a country wants to take down another country's power grid or critical infrastructure, there are brute force nonkinetic tools to accomplish the task. However, the consequences are akin to General William T. Sherman's march to the sea. If the nondiscriminate attack is cyber based, the attacking country may inadvertently violate numerous sovereignties as it applies the tool. Ultimately, the negative collateral effects of a broad-brush, nonkinetic attack may be worse than the original problem that precipitated the attack.

However, in the realm of surgical, nonkinetic targeting, Sun Tzu's words are as applicable today as they were when written in 500 BCE. The key word is *surgical*. In such an attack, a specific target is affected, in a manner that may be nonattributable, for a predetermined duration that limits collateral damage. As stated by Sun Tzu, a successful surgical attack has the potential of subduing the adversary without endangering the warfighter or innocent civilians. As this article demonstrates, surgical nonkinetic targeting requires an art form called forensic vulnerability analysis. With more than 20 years' experience as a forensic vulnerability analyst, targeteer, and warfighter, I can attest to the value of forensic vulnerability analysis in uncovering and targeting advanced terrorist planning, finding and fixing high-value assets, protecting the supply chain of national security systems, creating courses of action that maximize effectiveness and minimize negative collateral effects, and enhancing all areas of traditional campaign planning. However, its use and value have been kept in the shadows, and this lack of visibility is having dangerous consequences.

In discussions with Intelligence Community leadership, DOD planners at the combatant commands and Joint Staff, and leaders at many of the national laboratories, forensic vulnerability analysis is an art form that seems to be on the last stages of life support. In these organizations, the majority of remaining forensic vulnerability analysts are approaching retirement age. Compounding this problem is a lack of a training program to challenge, incentivize, and mentor the tech-centric next-generation warfighters to become forensic vulnerability analysts. The purpose of this article is to sound the alarm that the expertise necessary for successful surgical nonkinetic targeting is about to become organizationally extinct, and unless the problem is addressed, the art of war will become the science of war.

Forensic vulnerability analysis uses established auditing principles, due-diligence protocols, operational security survey methodologies, and exhaustive research of peer-reviewed documents to build awareness of obvious and non-obvious relationships and linkages. Then forensic vulnerability analysis leverages trusted relationships with recognized subject matter experts in industry, academia, and governments to transition and characterize the linkages into obvious and non-obvious vulnerabilities, identify and mitigate negative consequences, and establish a process to collect and measure effectiveness. As an aside, the non-obvious vulnerabilities often produce the most favorable effects with the most limited negative consequences. Sometimes these vulnerabilities appear separate from the primary target by commercial mergers and acquisitions, joint ventures, layered boards of directors, government advisory service, venture capital, shell corporations, third-party integration, and so forth. From experience, the most critical vulnerabilities exist at 3 to 4 degrees of separation from the target. I have found that 4 degrees of separation from the target of interest usually encompass the majority of critical vulnerabilities.

For those unfamiliar with the concept of degrees of separation, consider this scenario. A targeteer is attempting to discover a critical vulnerability in Company V, which produces a weapons system that could jeopardize U.S. national security. In the production of the weapons system, Company V receives electrical power from a hydroelectric system owned by Company W (1 degree of separation). The hydroelectric system uses turbines supplied by Company X (2 degrees of separation). The turbines are controlled by an electrical management system supplied by Company Y (3 degrees of separation). Company Y subcontracts the development of the configuration files to Company Z (4 degrees of separation). This analysis of linkages is accomplished not only for the production process, but also for the leadership, supply chain, financial, geopolitical, and cyber processes. Once these relationships are known, subject matter experts empower the targeteer so that a surgical nonkinetic attack against Company Z ripples up to Company V, accomplishing the national security objective.

In DOD capstone documents Joint Publication (JP) 3-0, *Joint Operations*, JP 2-0, *Joint Intelligence*, and many other joint publications and Service planning documents, the concept of a target system of systems is described verbally and portrayed graphically. Figures 1 and 2 from JP 2-0 portray the system-of-systems concept.

The figures portray a linear relationship matrix. Once the relational linkages

Figure 1. Identifying Centers of Gravity

Source: Joint Publication 2-0, IV-14.

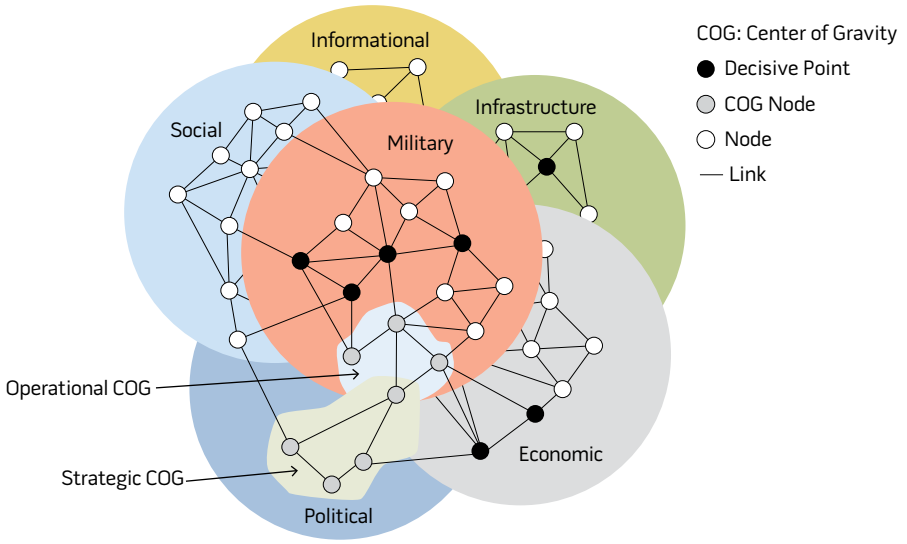
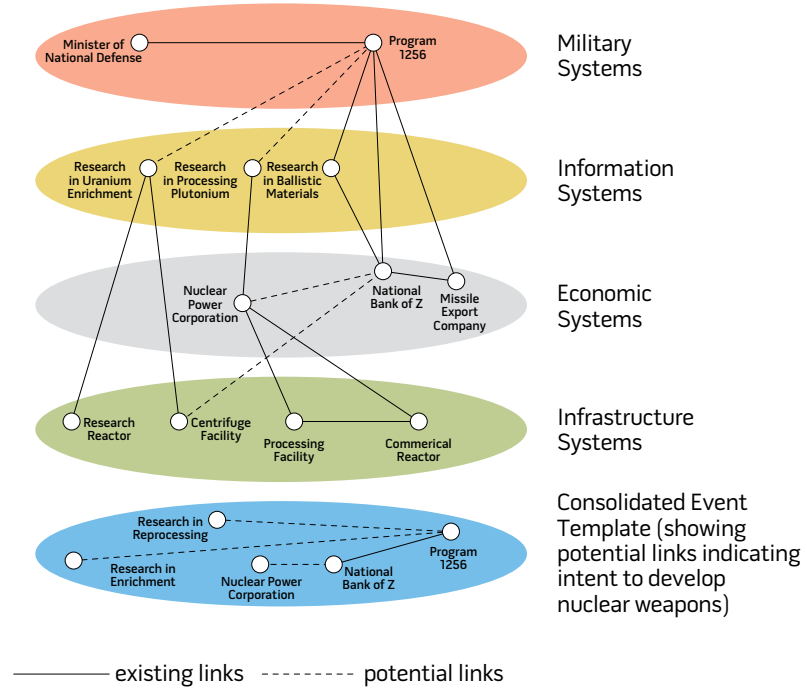


Figure 2. Systems-Oriented Event Template

Source: Joint Publication 2-0, IV-15.



are known, targeting is accomplished to elicit a desired and measurable effect toward achieving the stated campaign objective. The system-of-systems concept is not new. In World War II, the Allies targeted ball-bearing plants in Schweinkurt, Germany, to affect German aircraft production. During Operation *Desert Storm*, Iraqi power plants were attacked to negatively affect Iraqi defensive capabilities. The system-of-systems concept remains valid; however, the world is more complex now than at any time in history.

In today's interconnected, multinational world, the current DOD figures do not adequately portray reality. If the traditional, linear relationship methodology is used to target in a complex, interconnected, multinational world, the targeteer has the likely possibility of providing the joint force commander with courses of action (COAs) built on incorrect assessments of risk versus effectiveness. One reason for an incorrect assessment is that traditional nodal analysis defines criticality of a node via the number of linkages and analysis out to 1 to 2 degrees of separation. For example, if Company V has two critical nodes, one node with 100 linkages and one node with 2 linkages, common knowledge dictates that the node with 100 linkages must be the most critical. However, imagine that the 100 links were employees linked via social media, and the other nodes 2 links were actually the leadership and command and control networks. Now which node is more critical?

The underlying problem is that to be effective in a surgical nonkinetic strike, the targeteer needs to realize that the system of systems is a culmination of multinational, multilinked, multitiered, and non-obvious sub-targets. All that the world sees is the primary target, but in reality, the target is a culmination of numerous symbiotic units. For example, an aircraft is no longer produced at one plant. In the case of a next-generation fighter jet, there may be thousands of contractors and subcontractors all providing numerous components, any of which could jeopardize the aircraft if compromised. In the case of a power grid, there are thousands of substations, each with thousands of components that can be used to collapse the grid at any given time. Many of these subtargets are multinational. Many have nodes that are U.S. entities, which adds complexity in regard to authorities. Some of the nodes may cross established U.S. Government organizational areas of responsibility with conflicting authorities. Most nodes have critical information that is not accessible via established government collection capabilities.

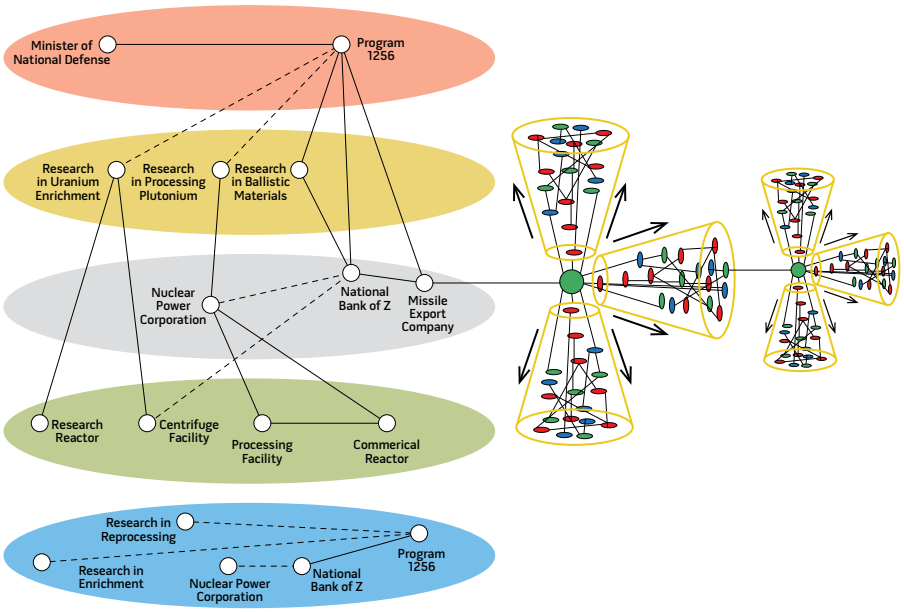
The bottom line is that in a complex, interconnected world, a targeteer cannot accurately determine a critical target

outside of a forensic vulnerability analysis that identifies both obvious and non-obvious relationships.

Figure 3 updates figure 2 to make it relevant for today's targeting solution. For the purpose of an example, the graphic identifies a missile export company in the economic tier. Traditional nodal analysis will look at the company and how it fits with the national security objective (for example, remove country X's capability to export nuclear ballistic missile airframes, warhead components, and related technology to country Y). Traditional analysis will look at the flow of money, company leadership, connectivity to other identified nodes, and so forth. The nonkinetic COA may be to infiltrate the shipping dispatch network and route the shipment of missiles to another location, thereby accomplishing the national security objective. However, this solution looks at a complex scenario through a simplistic lens and creates a logistics quagmire with potentially global negative effects. For example, if the attack is successful and the vessel transporting the missiles is rerouted, what about the other legitimate commerce on the transport vessel? That vessel is also scheduled to pick up additional legitimate cargo at the original destination (second cluster in figure 3). If the rerouting is successful, the uncertainty infused into the shipping industry drives up shipping insurance rates exponentially. This cost is handed off to the customer. Ultimately, these increased costs of business affect the ability of the multinational shipping company to conduct competitive commerce, which creates additional global issues (third cluster in figure 3).

From experience, senior government and DOD leaders understand these inherent complexities, which make them historically unwilling to accomplish surgical nonkinetic courses of action presented as part of a campaign plan. Even if these COAs religiously follow established planning doctrine to include intelligence preparation of the battlespace and are exhaustively wargamed, the commanders will know that a wargame of faulty assumptions creates faulty COAs.

Figure 3. Interconnected and Global System of Systems

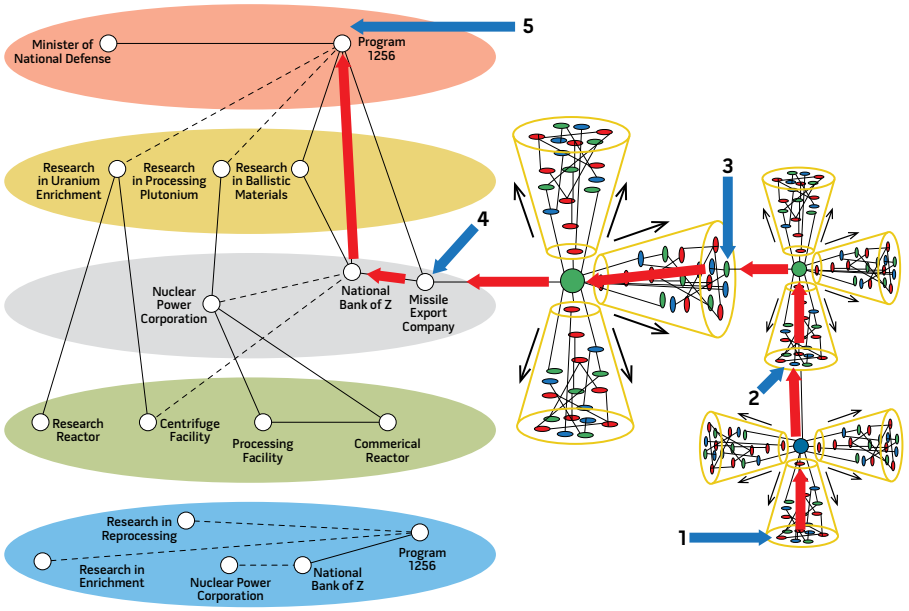


However, forensic vulnerability analysis is optimized to identify links and relationships that are usually hidden. In the previous missile export company example, the forensic vulnerability analysts would start where the traditional planners using the methodologies in figures 1 and 2 stop. From that point, the missile export company's leadership, corporate papers, and financial health would be analyzed. The leaders probably occupy leadership positions in the government, other corporate boards, or civic institutions. Each of those entities is analyzed. The banks that move the company's money are analyzed down to 4 degrees of separation. Analysis includes leadership and corporate linkages (such as joint ventures, subsidiaries, and shell companies). The shipping and dock worker companies are analyzed, as are the systems used for dispatch and all the components and companies that sell the components comprising the dispatch system. The company that transports the missiles to the dock is analyzed. The company that picks up the missiles at the desired end point is analyzed. Ultimately, the system-of-systems graphic that the traditional targeteer uses (figure 2) becomes the system-of-systems that the forensic vulnerability analyst creates.

Although complex in appearance, the links and nodes are characterized by critical and intimate information supplied via the forensic vulnerability analyst's trusted relationships in the private sector, academia, and government. Interactive wargaming provides the commander with an important "what if?" capability. Using the previous example of the missile export company, the forensic vulnerability analysis, subject matter expertise, and associated interactive wargame could produce a course of action as shown in figure 4.

The following are linked forensically: Country X's nuclear ballistic missile program (5) uses the named missile export company (4) to move airframes, warhead components, and critical technology to country Y. The leader of the missile export company has a trusted relationship with Freight Forwarder A (3), which uses an international bank (2) that has a branch in country Y. This bank (2) has a board of directors with one director who owns a freight insurance company (1), the same company that provides insurance for the export of the missile shipment. As a result of this forensic vulnerability analysis, targeteers could surgically attack the system in such a way that the export company does not receive the necessary letter of credit and insurance. Granted,

Figure 4. Forensic Vulnerability Analysis Used in Surgical Nonkinetic Targeting



following the COA is not as flashy as launching a Tomahawk; however, the result still keeps country Y from receiving the nuclear ballistic missile system.

The cadre of forensic vulnerability analysts is dwindling due to retirement and routine attrition, and there are few to no replacements. A national lab leader recently concluded that forensic vulnerability analysis is an art form in danger of extinction. Unfortunately, as an art form, there is no present means to automate the forensic vulnerability analysis process. The problem is that much of the analysis is interpretation based on years of experience. In the future, an artificial neural network may be created that can successfully accomplish forensics. However, if such a network is created, it would still require experienced forensic vulnerability analysts to assist in the network's "learning."

The Department of Defense and Intelligence Community need to address the issue of a dwindling forensic vulnerability analyst cadre before it reaches a point of no return. There needs to be a dedicated training and recruiting effort to identify motivated warfighters. There needs to be a symbiotic relationship with academia and industry to provide unique mentoring opportunities for the trainees. There also needs to be a dedicated career path that accounts for the longevity of specialization required to produce an expert forensic vulnerability analyst. The good news is that there are enough experienced analysts to act as instructors and mentors, and there are cooperative research and development agreements in place to leverage academia and industry. The bottom line is that this cadre death spiral can be rectified with little funding, but commitment to action needs to be made in the short term.

This article seeks to bring awareness to a unique specialty in the Department of Defense and Intelligence Community: forensic vulnerability analysis. It has stayed in the shadows since the birth of the Nation and has been instrumental in the success of many of the greatest U.S. campaigns. It is truly the "art" in the art of warfare. However, out of sight has also meant lack of attention. As the world becomes more tech-centric, there is an inadvertent momentum to make warfare more scientific. Unfortunately, the more technologically complex the world becomes, the more critical the art of forensic vulnerability analysis will be to protecting U.S. national security and safeguarding the warfighter in harm's way. It is time for DOD and the Intelligence Community to make changes to strengthen this discipline and bring the art back into the art of war.

Addendum: Forensic Vulnerability Analysis Case Study

The following is a real-world case study in which forensic vulnerability analysis was used to uncover the end stages of terrorist planning and was instrumental in validating and subsequently terminating the threat. In a touch of irony and future concern, the U.S. Government's forensic vulnerability analysis effort uncovered al Qaeda using a crude form of forensic vulnerability analysis as part of its targeting process.

Overview. On April 15, 2004, Osama bin Laden released an audiotape giving Europe 3 months to leave Islamic countries or face renewed attacks. By August, the 90-day deadline ended. However, based on information gleaned from a seized laptop, the U.S. Government and Intelligence Community were not looking at Europe but were preparing for an al Qaeda attack against one of five financial centers in the United States.

Early Warning from Academia. A leader from an academic organization read an article in a newspaper from Milan, Italy. The author of the article was known to the academic (2 degrees of separation) and had a track record of unique insight into the workings of al Qaeda. In the article, the author stated that al Qaeda would not attack the United States. The attack would be against Europe to punish the countries for ignoring bin Laden's 90-day truce. He went on to state that his sources (3 degrees of separation) indicated that the attack would occur in one of five cities to include London, Rome, and Paris. Because the academic was part of a forensic vulnerability analysis trusted relationship network, this information was pushed by the academic to a DOD forensic vulnerability analyst.

Early Warning from Industry. At the same time, a global investment banking leader, also in the trusted relationship network, notified the same

Joint Cyber Analysis Course instructor at Information Warfare Training Command Corry Station helps high school student complete cybersecurity challenges during third annual CyberThon event at Naval Air Station Pensacola, January 21, 2016 (U.S. Navy/Taylor L. Jackson)

DOD analyst of interesting dialogue in financial blog sites. The banking leader stated that a particular financial blog produced a disturbing thread. A blogger posted a question asking how an entity could collapse a nation-state's economy. Other bloggers answered to forgo attacking structures and focus on attacking economic leaders. The bloggers went on to say that al Qaeda planned incorrectly when they attacked the World Trade Center; what they should have done was attack the stock exchange leadership and traders. (Note: This is a perfect example of the value of forensic vulnerability analysis [target finance leaders] versus traditional nodal analysis [target the building]). This blog thread demonstrated al Qaeda's crude attempt to accomplish forensic vulnerability analysis.

Forensic Vulnerability Analysis. The DOD analyst started an effort to determine if the academic thread was linked to the financial thread. An additional benefit of a trusted relationship network is that the network can find a singular expert out to 4 degrees of separation. In this case, the analyst was directed to a finance expert familiar with the five European locations. He took part in a red team exercise hosted by the analyst. He was asked to put himself in the place of the terrorists and stage an effective attack against economic leaders. When asked, "In what European city would you stage the attack and how?" the leader responded that because of close-hold information that he was privy to, he would attack a "specified location" in London with either a chemical/biological weapon or a hijacked airliner. A successful attack in that area would cripple the United Kingdom for years.

Corroboration from the Intelligence Community. Intelligence databases were queried for the subject of al Qaeda in London—the "specified location"—and airliners. Message traffic identified an al Qaeda cell, but not much else was known. However, the DOD analyst was able, via non-obvious relationships and trusted subject matter expertise, to link the academic information, business information, expert red team, and intelligence traffic. The result was actionable intelligence with increased fidelity and probable intent. The complete forensic vulnerability analysis process took 48 hours from initial message to research completion.

Actions Taken. The data, forensic nodal analysis, and corroborating intelligence were given to the United Kingdom liaison at DOD. In post-event talks in London between the United Kingdom's cabinet secretariat, the ministry of defense, security services, the Joint Terrorism Analysis Center, the DOD analyst, and the banking leader, it was learned that the al Qaeda unit members were arrested before they could execute their plan. Of note, the al Qaeda unit was known to the British authorities and they were actively monitoring the unit's activities. The forensic vulnerability analysis added fidelity to the United Kingdom's case for action. Information learned via interrogation confirmed the findings of the forensic vulnerability analysis. JFQ