The Implications of Virtual Deception

by

Lt York W. Pasanen

Introduction

As the dawn breaks across the western Atlantic Ocean, two F-25 Virtual Attack Fighters (VAF) takeoff from Seymour Johnson Air Force Base. Captain Bjork Williams and Robert Oehlke find themselves flying another standard combat air patrol along the East Coast. Recently, terrorist groups have acquired late 20th century U.S. Navy Aegis cruisers and have been conducting raids upon the new Border states of the Virgin Islands and Bermuda. As the two aircraft make their way out to sea, clouds begin to roll in and the ocean surface is quickly obscured. Approximately twenty minutes into the mission, a surface vessel is picked up on the multi-spectral imaging and sensor system abroad the F-25's. Even though the target is identified as a fifty-foot catamaran, the two pilots decide to buzz by and take a look. As they break through the clouds the pilots realize something is drastically wrong. Three Aegis cruisers appear before their eyes, while their computers still show only a small watercraft. Hackers aboard the cruisers tapped into the F-25 imaging system and altered the information processed within the systems. Before the pilots can react to the trap, their aircraft are shot by a short-range electro-magnetic pulse weapon, and fall powerless into the sea. Captains Williams and Oehlke have just become victims of Virtual Deception.

Welcome to the year 2025. By now, information and its control are the power and status symbols. The boundaries between nations are no longer territorial points guarded by massive armies, but supercomputer switching stations welcoming all people with their virtual messages. Cyberspace is the dominant dimension in warfare, and those who control it (nations, corporations, or individuals) are the superpowers. Several international powers have access to networked multi-spectral imaging and sensor systems. For the first time, all participants have a clear view of the battlespace and the assets available to every opponent. Systems and processes have advanced to the point where the shooter receives real-time information about all actions and assets in the battlespace environment. According to some experts, "We have reached a point where technology which supported combat has become a weapon in its own right" (Ryan 114). The shooter literally sees a complex 3-D chess game where opponents can attack from anywhere. This awesome capability of delivering real-time processed information to the shooter or higher levels of hierarchy has opened the door for the ultimate form of information warfare. Virtual Deception will require the U.S. military to alter its paradigms about warfare, and hence make sweeping changes in its doctrine, force structure, and military strategy to be ready for warfare in 2025.

Virtual Deception & the World at 2025

Virtual Deception is the new warfare tactic coming of age, and is by far the most damaging warfare practice in the year 2025. I define Virtual Deception as follows:

> the use of network communication/information system to shape the enemy's view of the battlefield by deliberately and explicitly altering, distorting, blocking, or destroying the real-time information processed in the enemy's imaging and sensor systems with the intent of deceiving the enemy to behave in a predetermined manner, and thus indirectly control the enemy's actions.

Since the turn of the century technology has advanced at a mind-numbing rate. Technology such as bistatic sensors, 3-D holographic DNA storage, and artificial omnisensory sensors developed during the early twenty hundreds have enabled the standard 3-D Multi-Spectral/Omnisensoral imaging systems present in 2025. In addition, the civilian sector development and perfection of real-time video insertion and terahertz communications system increased the speed of the decisionmaking process dramatically. The predictions of the destabilization of the global community were correct, and all conflicts in 2025 are limited in duration, involve coalitions, and aim at restoring regional stability. Due to the explosion of information gathering and processing systems, almost anyone can participate in shaping the global environment. However, the inability to place restraints on access to the global community is still a serious weakness.

Possibilities of Virtual Deception

Virtual Deception strikes at each of the four methods of intelligence/information gathering: Open sources; IMINT; SIGINT; and HUMINT. The corruption or compromise of this data involves the direct or indirect attack of a target system and obtaining full or partial control of that system. The rapid expansion of the web/net and the military network of communications/ information system will give the United States a distinct advantage in future conflicts. A fully integrated network of satellites, C4I, aircraft, ground, and naval forces is on the horizon. As early as 1998, F-15's will be equipped with a digital datalink to provide a real-time electronic order of battle (Cook 49). This program is part of the pentagon's future strategy to, "overwhelm the enemy with technical superiority and aircrew knowledge . . ." (Cook 48). However, our future dependence on information and information systems, although an advantage, will also be an inherent weakness. Our current lack of network security has already indicated several problems with our future information dependency. According to the Defense Information Systems Agency (DISA), hacker attacks on the Pentagon itself are now running at two per day (WSJ 20).

The scariest prospects are the new software programs that act as hardware. These micro-programs are designed for the one-time use of an application and have the capability of e-mail distribution. Numerous software producers are currently researching this possible technology. The implications of these compact, disposable, and untraceable programs are endless. Cruise or sleeper viruses could easily be incorporated into such programs, enabling unauthorized access to any information the hacker desires. At this point, Virtual Deception becomes a significant concern.

Capabilities of Virtual Deception

Virtual Deception is by no means a new concept. In fact its roots are centuries old and can be traced back to Sun Tzu who stated, "the primary target is the mind of the opposing commander", and, "all warfare is based on deception" (Sun Tzu 41). Virtual Deception takes the principles

envisioned by Sun Tzu and combines them with the capabilities of modern technology. The result is a psychological warfare concept based on the reflexive control of the enemy decision cycle. According to Dr. Tim Thomas of the Foreign Military Studies Office, "Reflexive control involves creating a pattern or providing partial information which causes an enemy to react in a predetermined fashion without the enemy realizing that he is being manipulated" (Thomas 13). The ultimate goal of Virtual Deception is to deliberately manipulate information to deceive the opposing commander to make a decision predetermined and desired by the opposing side. Dr. Tim Thomas has conducted in-depth research on the theory of reflexive control used by the former Soviet Union, and he uncovered the writings of Vladimir Lefebvre, one of the best Soviet minds working on Reflexive Control. Lefebvre believed, "We [the Soviet Union] can influence the channels of information and send messages which shift the flow of information in a way favorable to us" (Reid 293). In addition, he also listed several types of reflexive control that could be exploited by Virtual Deception. They are:

- transfer of an image of the situation: providing the opponent with an erroneous or incomplete image of the situation.
- creation of a goal for the opponent
- form a goal by transferring an image of the situation: creating a false picture
- transfer of an image of one's own goal: a feint (changing the enemy's perception)
- transfer of an image of one's own doctrine (false view of decision-making procedures)
- transfer of one's own image of a situation to make the opponent deduce his own goal
- reflexive control of a bilateral agreement by a third party
- reflexive control over an opponent who is using reflexive control: exploiting opportunities
- identified as imitation of the initiators own process of reflexive control (Reid 296-308).

Using Virtual Deception, each of these reflexive control theories can be applied in the warfare of 2025. The manipulation of a few bits of information in an enemy's information processing system can make the enemy see friendly military assets that do not even exist. This concept I call Virtual Deterrence will be addressed later. A good example of this deterrent capability is illustrated by the possible compromise of the U.S. Army's "All Source Analysis System." According to the U.S. Army, this system will someday, "fuse threat information from all intelligence disciplines and provide correlated intelligence to maneuver commanders and staffs down to battalion level" (www.army.mil). The consequences of the enemy manipulating the system which will handle ninety percent of the Army's intelligence could change the result of the war or prevent it from happening. Similarly, Mr. Jim Cooper, a senior analyst at the Air Force Information Warfare Center: Concepts Division, stated the use of such methods and technology against U.S. classified information systems could provide a "stepping stone" to other classified networks and, "could severely affect the flow of intelligence" throughout U.S. military systems (Cooper Int).

Another possible manipulation is attacking the enemy's media to alter the enemy's perception of the global environment or transpiring events. In the Tofflers' book entitled War and Anti-War, "the most powerful mind-wrench of all is meta-propaganda -- propaganda that discredits the other side's propaganda" (168). The result is the swaying of public or political opinion within the enemy nation, which is a powerful weapon. The consequences of using meta-propaganda against

the U.S. are drastically increased due to our open democratic society. Also since the media is the watchdog of the government, the manipulation of the watchdog could wreak havoc for our government.

Lastly, the ever-increasing capabilities of satellite reconnaissance can be countered without the political upheaval of destroying a foreign satellite. Since most nations believe in the vehicular sovereignty of satellites, the destruction of one is liable to prompt a declaration of war. However, Virtual Deception techniques could be used to manipulate or leech the data traveling through the satellite itself without the enemy knowing about the intrusion. All of these possibilities have significant ramifications for the military of 2025.

New Missions for the Military of 2025

According to Lt. Colonel Donald Ryan, Jr., a USAF communications officer, the capabilities of Virtual Deception can, "alter, interdict, or destroy information and information assets thereby determining the outcome of military operations" (116). In the near future, Virtual Deception, will be the precursor to conventional warfare, and fill similar missions as airpower does today by preparing the battlespace. In fact, the Defense Science Board believes the ability to wage information warfare, "may be the most important facet of military operations since the introduction of stealth" (Nation Defense 30). Thus, the U.S. military must change its current paradigm about the capabilities of information warfare and Virtual Deception, and begin adapting to its inherent capabilities and threats. Several new missions for the United States military can evolve as a result of Virtual Deception capabilities. Most of them will deal with managing perceptions and manipulating information (Thomas 15). Some possible missions include:

- Virtual Interdiction: Using computers, programs, or viruses to interdict information traveling through the enemies satellites, information centers, and weapon systems.
- Counter Virtual Interdiction: Using computers, programs, and anti-virus systems to protect against compromising military information in satellites, information centers, and weapon systems.
- Virtual Deterrence: The Strategic use of Virtual Deception to transfer a false image of the situation, one’s own goal, or one’s own doctrine to force deterrence upon an opponent.
- Strategic Virtual Attack: A direct attack upon an enemy’s information processing or collection systems through the use of programs, virus, etc. to destroy, blockade, or capture information within or passing through the systems.
- Tactical Virtual Deception: Tactical applications to virtually deceive the persons or computers operating sea, air, or land weapons systems (i.e. the F-25’s in the introduction)

Each of these missions may have several unique applications for the U.S. military. Several more specialized missions could evolve from the ones I have defined above. As an unnamed Russian Army officer stated in a 1990 unpublished article, "The goal of warfare in the information age is to seize and to hold control over an adversary’s information resources (as a main kind of national resource) and through them - over the rest of his resources" (Thomas 16). Thus any method achieving this goal has possible military applications. However, it’s unrealistic to assume only the United States will have the capabilities to wage such warfare. Non-governmental

organizations such as organization crime groups (Mafia), drug cartels, religious or political fanatic organizations, etc. could also gain the capabilities necessary for Virtual Deception. Thus, a revolutionary change in our doctrine and eventually organization must occur to adapt and exploit Virtual Deception and prevent our enemy's from deceiving us.

New Doctrine

Major Robert Steele (Ret), a former United States Marine Corps officer, summed up U.S. policy on changing doctrine in his article entitled "Transformation of War and the future." In his article written while still on active duty he states, "We as a nation have a tendency to try to fit reality to our force structure" (Steele). Changes in the military especially when they pertain to changing doctrine have never been accepted well. However, the current revolution in military affairs will change the way the military fights in future conflicts. The threat of Virtual Deception capabilities by any enemy poses a major task for our military in the future. The U.S. must begin to incorporate Virtual Deception doctrine into the national and military doctrine, (1) To protect vital strategic national assets, (2) Monitor those who threaten or use Virtual Deception, (3) Enable the U.S. to efficiently and effectively use Virtual Deception against its enemies. However, before this doctrine can be created and understood, three basic questions need to be answered: "When does war begin?"; "How should war be fought?"; and "How will we define victory in the future?" (Ryan 115). Virtual Deception changes our current paradigms for answering each of these questions. The first question poses a difficult task for the senior leadership of the U.S. A declaration of war is unnecessary for Virtual Deception since it concentrates on waging a secret war against an adversary. We must determine how we will respond to the use of Virtual Deception on our information and our information gathering systems. Academician V.I. Tsymbal already stated how Russia will react to nations using information warfare against Russia:

> From a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not...considering the possible catastrophic consequences of the use of strategic information warfare means by an enemy, whether on economic or state command and control or on the combat potential of the armed forces...Russia retain the right to **first use nuclear weapons against the means and forces of information warfare, and against the aggressor state itself** (Tsymbal 7.)

Thus the U.S. has a considerable problem to solve: How to proportionally respond to enemy use of Virtual Deception? Our retaliation can range from political pressure to nuclear weapons usage. Nonetheless, the U.S. must begin to deal with this issue now before the situation is forced upon us.

The second question of how to fight wars once again addresses how the U.S. will respond to enemy use of Virtual Deception. If information is considered a strategic national asset, then any use of Virtual Deception against the U.S. would be considered an act of war. However, if current doctrine and policy are kept, Virtual Deception, so long as it is non-lethal, will not be considered a threat to our national security (Ryan 115). Thus, we will be subject to devastating "legal" VD attacks. Our paradigms regarding the use of Virtual Deception must evolve to incorporate all

aspects of VD attacks. Currently, our military doctrine is focused upon large scale physical engagements. I postulate that future military doctrine must develop a new strategy prepare the military of 2025 for the increasing intensity of VD attacks. Many enemies of the United States will soon gain access to limited VD capabilities. Without the insight to see how Virtual Deception will affect our nation and military in the future, our limited paradigms will force us to face disastrous consequences.

The last question has a direct impact on the future of the military. The revolution in military affairs will drastically change the way victory is achieved in the future. As stated earlier, the goals of Virtual Deception lie in the seizure and control of an enemy's information systems. In addition, a formal declaration of war is not required for Virtual Deception. Therefore, victory could be achieved not only without a declaration of war, but without the enemy even knowing they had lost! Once control of information resources is achieved Virtual Deception would come into full effect. False information and realities could be presented to the military, the politicians, and the public, and ultimately their decisions would be reflexively controlled. A nation, group, or individual could adversely affect major decisions within the U.S. and could become a virtual puppetmaster for decisions affecting everything from politics to the content of weekly television. Obviously, this is taking the concept of Virtual Deception to the extreme. However, to control its effects and survive in the unstable world of 2025, it is clear that our current national and military doctrine must change.

New Military Force Structure

The doctrine loop is a standard feedback loop composed of multiple inputs which directly relate to military doctrine and strategy. In addition, changes to doctrine and/or strategy are directly observed in outputs such as force structure. The last step in the loop is feedback which evaluates how effective our current doctrine, strategy, and outputs are keeping pace with ever-changing inputs. Threats are very important input to the doctrine loop and often force doctrine to change. However, if threats, doctrine, and strategy change, so must the U.S. military force structure. Currently the U.S. force structure is organized to deploy and engage in corps sized forces in no more than two major regional conflicts (MRC). However, as seen through the prior analysis of future threats, Virtual Deception will enable small elite groups to wage war against nations. Similarly, analysts at the National Defense University stated, "small numbers of specialized highly capable systems can provide the edge over classical forces in a conflict" (www.ndu.edu) In addition, the trends in the revolution in military affairs show the decreasing dominance of large weapons platforms, and place more emphasis on information gathering and processing systems. In an interview with Dr. Tim Thomas of the Foreign Military Studies Office, he stated the U.S. military organization, "should be aimed towards the detection side" to protect our vital national asset: information. Several opinions by experts throughout the U.S. have been expressed on how the U.S. military force structure of the future should look. There are numerous possible ways the U.S. can adapt to best exploit the RMA and Virtual Deception. Some of these include:

- Establishing an Information Corps (Hazlett 88)
- Establishing an Information career field within the Operations career group
- Virtual Deception Special Operations Teams

- Information Warfare Squadrons: Attached to every wing sized organization and under command of USSPACECOM due to its large capacity for information gathering.

Each option has significant positive and negative aspects. However, I will not debate which organizational method is the best. Although, one more organizational problem is worthy of mentioning. The legal aspects of Virtual Deception and other information-based warfare (IBW) methods are still to be decided. The U.S. legal system must soon establish laws on network security and violations thereof. In addition, a national organization, possibly with a cabinet position, may be required to handle the political, legal, and administrative aspects of Virtual Deception and IBW. Although several options have been expressed, the question of how to best organize the U.S. military to use Virtual Deception offensively and how to defend ourselves from its use still remains to be answered.

Conclusion

Through my analysis, I have examined the possibilities and capabilities of Virtual Deception, as well as the consequences for changing U.S. national and military doctrine and force structure. Although 2025 still lies thirty years down the road, the prospects of Virtual Deception and other methods of IBW will soon become reality. Consequently, the U.S. military must be ready to adapt to the threat Virtual Deception poses, and must prepare to use it against future adversaries whether large or small. Current paradigms about how war is conducted must change to exploit the RMA and Virtual Deception. Our current military doctrine and force structure must also change, lest our country fall prey to the nemesis of Virtual Deception. However, one question remains unanswered: How will the U.S. military change to cope with the ultimate form of IBW: Virtual Deception.

Work Cited

"Army's All Source Analysis System" Online. Internet. 2 Dec 95 Available: http://www.army.mil/pmif-pg/asas.html

Cook, Nick. "Data and Stealth Key to Air Attack." International Defense Review. November 95: p 48-52.

Cooper, Jim. Air Force Information Warfare Center, Concepts Division. Telephone interview concerning the possibilities and capabilities of Virtual Deception, and its effect on Air Force Information Systems. 5 December 1995.

Hazlett, James, A. "Do we need an Information Corps." Joint Force Quarterly. Autumn, 1993: 88-97.

"Information Warrior Raze Enemy's Vital Data Chains." National Defense. March 1995: 30-31.

"Pentagon studies art of 'information warfare' to reduce its systems vulnerability to hackers." Wall Street Journal 3 July 95: 20.

Reid, Clifford. "Reflexive Control in Soviet Military Planning" Soviet Strategic Deception. ed. Brian Daily and Patrick Parker, Lexington Books, Hoover Institute Press: 293-311.

Ryan, Donald E. Jr. "Implications of Information-Based Warfare." Joint Force Quarterly. Autumn/Winter 1994-95: 114-116.

Steele, David. "The Transformation of War and the future of the Corps." (28 April 1992) n. pag. Online. Internet. Available: http://gopher.well.sf.ca.us: 70/0/Military/Intelligence/futwar.txt

"Strategic Assessment 1995: U.S. Security Challenges in Transition." National Defense University. Online. Internet. 2 Dec 95 Available: http://www.ndu.edu/ndu/inss/sa95/sa95cont.html

Sun Tzu. "The Art of War." ed. Samuel Griffith. New York: Oxford University Press, 1963.

Thomas, Timothy L. Foreign Military Studies Office, Fort Leavenworth, KS. Phone interview concerning Reflexive Control and its possible applications in Virtual Deception. 21 November 1995.

Thomas, Timothy, L. Russian Views on Information-Based Warfare. Fort Leavenworth: Foreign Military Studies Office, 20 September 1995.

Toffler, Alvin, and Heidi. "War and Anti-War: Survival at the dawn of the 21st century." Boston: Little, Brown and Company, 1993.