Fourth Generation Warfare Tactics: Are Police Operationally Ready?

International Police Executive Symposium
Aug 8th– 13th, Washington DC

Tino Posillico, Ph.D.
State University of New York at Farmingdale
Dept of Criminal Justice
Dept of Security Systems and Law Enforcement Technology
United States of America

Abstract

As some security scholars recognize, we are now into the 4th generation of warfare evolution. Although police traditionally have not been at the frontline of warfare activities, the latest generational viewis departing from that long-held position and is critically impacting the tactics of police operations. Armed forces and law enforcement have been slowly adapting to this latest shift, but it is not clear if the operational readiness is at a level needed to meet the newest challenges that have developed in this latest phase of a warfare activity. This paper addresses the implications of these changes and what role police ops may need to play in the adjustment of security strategies in the new generational view. Modalities of the shift will identified and a review of current policing relevancies in relation to the new generational developments will be explored and investigated. In particular, comparative features of reactive police ops versus interdiction ops will be applied to the requirements of the new generational characteristics. Finally, a summary of new initiatives and recommendations will be discussed as well as resource allocations needed to meet the latest challenges.

Keywords: Police, Operations, Warfare, Interdiction

Background

The generational view of the evolution of warfare spans some 300 years of development and was first proposed by Lind et al (1) and later updated by Hammes (2). While at least one source in the literature (Echevarria (3))questions the structure and application of the generational view- it appears to be widely accepted across most disciplines (Thornton (4), Friedman (5), Schmitt (6), Arquilla et al (7) and Ghanshyam (8)). A brief overview of each generation is presented here only for perspective—but the focus of this paper will be on the current stage of the evolution.

The 1st generation is characterized by very old style columns of soldiers consisting of close-order formations that were tightly supervised by the field command. This was typical of engagements seen in the American Revolutionary War and as well as the US Civil War. The literature implies this style of warfare was a hold-over from even earlier eras when battles were conducted with close-range weapons like swords and lances or were subjected to bows and arrows at an inaccurate range that could easily be deflected by shields or metal amour.

In the case of the 2nd generation, warfare was still a matter of linear tactics and movements of well ordered formations engaged in well-fortified lines of battle. The difference here was the development and use of long range artillery and early use of air power which were used to break the ranks of the enemy and allow an opening to be established to out-flank the enemy.

For the 3rd generation, a portion of the designated armed forces is directed to by-pass the direct battle front using superior weapons technologies and tactics like the use of para-troopers, missiles and air-borne delivery of hi-yield bombs to attack both rear military and civilian targets, thereby opening multiple fronts of battle and causing civilian casualties that can affect the domestic support of the war—both in production and on psychological levels. Early examples of this type of warfare can be seen in the prosecution of many battles of World War II – in the targeted use of bombing raids by the Allies, by the use of the V1 and V2 weapon attacks by the Germans Axis and also by the dropping of nuclear bombs on the civilian populations of Japan. There was also early glimpses of thebeginning of the next generation of warfare here as the Japanese Axis forces began to revert to the use of select Kamikaze attacks on the Pacific fleet of the American forces as the war began to wind down in favor of the Allies.

4th Generation of Warfare(4GW) Evolution

The next generation of warfare saw an intense development of sophisticated and complex weapons that could easily deliver hi-yield destruction to the enemy's homeland and civilian populations. These weapons included both tactical and strategic thermo-nuclear weapons, guided missiles launched from land or sea, and long-range bombers. Once these technologies became available, "super-power" nations began to employ them in their arsenals—although the United States had a strong lead in the research and development of these weapons, other nations were able to establish significant parity by the 1950's. Despite the emphasis on the sophisticated push-button weapon technology they employed, the super-power nations became reluctant to use such powerful weapons because of the doomsday scenarios they faced under the mutually assured destruction (MAD) scenarios that they now faced. Ironically, because of MAD, these nations now had to revert to more 3rd generation weapons usage to prosecute future wars and battlefield management. In fact, many of these nations began to look for other means to gain battlefield advantages and this shift reflected changes in ideas rather than technology. This shift away from "hot" sophisticated weapons began during the "Cold War" between the western superpowers and the eastern superpowers. This shift in the 4th generation approach focused on the strategic goal of collapsing the enemy from within his homeland, as opposed to any attempts to obliterate him completely through brute physical force.Gone would be the days of fighting the enemy in well-known and identified uniforms in simple linear actions—battlelines, battlefields and alliances would no longer be known or clearly labeled in a 4GW action.

Since the 1950's, the 4GW has developed slowly and steadily into a major force in modern warfare in today's global environment. It should be noted that the 4GW transition over the succeeding decades has been one of a "blend" of 3GW and 4GW approaches with 3GW on the wane as the new millennium began. Globally, 4GW has been a predominate mode of warfare in the 2010's that continues to gather support as it refines it's techniques and characteristics.

One of the earliest examples of a 4GW conflict was the Vietnam War of the 1960s. The very nature of this war typifies the 4GW action that has been seen in many developing countries. Right from the outset, this war's combatants were not readily and clearly recognized on many levels. Various elements of the French forces, US forces, Australian forces, Russian and Chinese operatives and as well as organized cells of local resistance (Communist Viet Cong) and allied forces (ARVN) were involved in military actionat one point or another. Historically, the involvement of some allied forces were termed a "police action" rather than a full-fledged military war.As the war expanded, the US and its allies prosecuted the fighting in 3GW fashion, while Viet Cong were waging more of a blended 4GW action. Indeed, the US and its allies won every major battle and conflict during the war due to their overwhelming 3GW superiority and dedicated armed forces– but later voluntarily withdrew because Communist forces also applied 4GW tactics including social and cultural propaganda affecting support for the war, guerilla style attacks and para-miltary operations within and among civilian domains. Unfortunately, after the US and its Allies voluntarily withdrew, the Communist forces went on to influence wars in neighboring Laos and Cambodia in a "domino effect" that led to dictatorial reigns of terror in those countries that eventually resulted in the murders of up to 3 million civilians by the Khmer rouge, the Pathet Lao and followers of Pol Pot.

A very similar example of a 4GW conflict involved the Soviet- Afgan War of the 1980s where Afgan resistance fighters employed hit and run guerilla warfare against Soviet forces in desolate and remote terrain areas that were very familiar to the Afgan forces who fought primarily as para-military operatives. As in the case with the Vietnam War, the Soviet forces eventually chose to withdraw ftom the area and abandon the war effort. It is widely believed that the impact of the critical failure in Afganistan led to the eventual break up and fall of the Soviet Union. Many historians refer to this conflict as the Soviet Union's Vietnam War (Cohen (9)).

Likewise, a final example of a 4GW conflict involves the US-led fight against the Taliban – a fundamentalist Muslim movement that became prevalent in the region after the 9-11 terrorist attacks by an earlier radical Muslim terrorist group Al Qaida took place in the US in 2001. Indeed, the Taliban followed the same 4GW combat doctrine that was outlined by a high ranking Al Qaida lieutenant in various briefings (Papyrus News, (10)). At the same time, the US was also waging aconflict inthe Iraq war which was enjoined by the US and its allies in a clear 3GW prosecution of the war. Once pushed out of Iraq at the end of that conflict in 2011, the Taliban retreated to the Afgan border to set up planned 4GW style attacks in quick cross-border retaliatory actions in Iraq which still continue to the current time frame of this paper.

4GW – Tactical and Strategic Deploymentby Hostile Forces

4GW Tactical Conflicts

At the onset of 4GWin the early 1950's, most occurrences of this new type of warfare generally were blended with more conventional 3GW style conflicts, where the 4GW forces played a supporting role in special cases where more conventional engagement would be difficult at best, e.g., the dense jungles of Southeast Asia. However, over the last 5 decades, 4GW tactical attacks have grown to become a predominate factor in the majority of global conflicts (WSJ (11)). Indeed, in many battle zones in northwest Africa and lower middle eastern regions, engagements have become dominated solely by 4GW tactics involving para-miltary activity and insurgent cells of localized militia that have multiple and overlapping affiliations (WSJ (12)). Yet, because none of these combatants have any clear and overwhelming superiority, these conflicts can sometimes carry on for years in a see-saw fashion – causing indefinite stabilization in the surrounding civilian areas. The good news is that most of these 4GW tactical wars can be halted by the direct and overwhelming 3GW intervention of any adjoining major military powers or their close allies. In the worst case scenario, where battle zones are remote and/or hold little or no strategic value, then safe zones can be created by major powers to isolate the 4GWcombatants and minimize civil collateral damage until the battle zone begins to shrink to the point where the combatants become mutually annihilated over time (Wash Times (13)). So in cases solely involving 4GW tactical combatants, overwhelming and intervening 3GW forces have been shown to be able to minimize the risk and vulnerability to adjacent civilian areas (Wash Post (14)).

4GW vs 3GWTactical Conflicts

In these type of engagements, the 3GW forces tend to dominate through most of the conflict. However, if the Powell Doctrine (World Political Review (15)) is not adhered to during the battle planning, the 3GW force's eventual victory will slowly revert back to the original adverse conditions which spawned the original conflict in the first case. This result is fairly consistent in case battles taking place over the last 5 decades: Vietnam, Soviet Union vs Afgans, US vs Afganistan, US vs Iraq and others (Jeffery Record(16)). So we see that engagements of these types must be carefully planned with a clear tactical goal as well as the final long term strategic plan to maintain the political stability and economic recovery and growth needed to support a democratic operation of the area or state. History tells us that strategic plans like these required major long term commitments (minimum 10 years) in both military presence and significant continuity funding to have just an even chance of being successful (J.E Armstrong (17)).

4GW Strategic Deployment

Strategic deployment by 4GW forces presents one of the most difficult types of attacks to defend by 3GW powers and their allies. This type of deployment can take many forms and include techniques which can be used in a variety of settings and locations, including homeland scenarios, which are fairly easy to plan and inexpensive to finance. It is this kind of action that transcends military scenarios and transfers the point of attack to local security and law enforcement. The elements of this attack provide the enemy with a reduced reliance on a central control and logistics system, creating independent compartmentalized units or cells which are typically seen in international terrorist organizations or domestic gangs and/or hate groups. These actions can result in damage to physical targets or personnel, as well as social and cultural objectives such as the reduced support for a particular war effort by the civilian population or economic instability or industrial power systems and infrastructure failure. This attack scenario is responsible for an increasing amount of the mass killings that take place in the US each year(LA Times(18)).

In all these cases, there is one critical factor that local police and law enforcement must be critically prepared for: the blurred distinction between civilian and military sectors and the absence of the traditional front or battlefield as well as the missing field command structure. Under these conditions, the risk/threat domain that must be observed is extremely broad and constantly expanding, making police coverage increasingly difficult.

However, analysis of the domains can provide simplification of the areas of hostile incidents. There are two branches of this type of deployment which need the most attention from local law enforcement:

***4GW Terrorist Activity* -** In this category, military bases, government institutions, police stations and private corporations are the frequent targets of the this action. Primary weapons are suicide-prepped operatives and/or car bombs and/or IEDs (improvised explosive devices). The suicidal aspect of these types of attacks have crucial impact on law enforcement response due to the irrational behavior of the perpetrator and the limited options for a non-lethal solution. Likewise, subsequent police investigations are negatively impacted by the suicidal factor since the "information trail" becomes problematic when the attack is completed and the perpetrator is deceased. The attacks at Foot Hood, the Naval Recruiting Center in Chattanooga and the Landover, Md police station are examples of this category.

***4GW Domestic Crime* –**This domain of 4GW includes traditional criminal profiles who have begun to adopt the 4GW approach in a domestic setting. Gangs, academic radical groups, extended protest movements (e.g., Occupy Wall Street, Move On, Black Lives Matter), rally ambushing of police personnel and even public sporting celebrations of major sporting events are all beginning to display characteristics of 4GW behaviors.Also, "Lone Wolf" and deep cover domestic terrorist operatives are highly decentralized and create major difficulties for police tracking any information about the clandestine and pre-operative action that is under way. The recent attacks in Kalamazoo, the Boston marathon, San Bernadino, Orlando and Dallas are examples of these scenarios.

Another important aspect of this category is its influence on young children who may be social "loners" and have a predilection to violent behavior. Taking a clue from 4GW-style attacks they may see or hear about in the media, they act out their aggressions in a copy-cat fashion to garner attention and/or exact revenge on other students. In many of these cases, the young attackers suffer from mental disorders that form the basis for their irrational action (Medical News Today(19)).

Comparative Review of 4GW Factors Influencing Effective Police Operations

While law enforcement is technically involved in all aspects of 4GW homeland attacks, this paper will focus on the domestic crime aspects of 4GW and how police operations are impacted by its strategies.

Goals of 4GW

As mentioned, the ultimate goal of 4GW is to inflict mass disruption, destruction and killing in as many point of attacks as possible. In a strategic domestic setting, this translates into a destabilization of civil and local order which can accumulate into a wider range of deterioration of services and lack of security.So in essence, the battle front that is emerging in 4GW is now transposed from the military battlefield to the civil, domestic and homeland areas. The question that has arisen currently becomes a matter of how police and law enforcement are coping with this transition and dealing with a quasi-military point of attack on their forces. It is clear that, on a historical basis, the 3GW capabilities of the western military forces and allies are superior to any others that are currently in the east. However, these modes of warfare, i.e., strategic troop movements, air and missile systems, close ground support, drones, etc….are totally ineffective in combating 4GW attack strategies. The same is true in the west's homeland defensive systems which are comprised of the same basic military weapons that are used in foreign 3GW engagements.

As a result, there is an urgent need for police and law enforcement operations to be re-evaluated in the expanding use of 4GW tactics world wide. Indeed, the growing wave of hostile operatives and agents being deployed domestically is a major concern for civil law enforcement (Washinton Times (20)), especially since these agents are well trained by hostile military forces that are usually well funded, have access to the latest weapons technologies and are sometimes isolated within sympathetic nations or nation states that refuse to allow western forces access to them. In addition, these hostile forces have well populated pools of recruits available to form a virtual endless supply of single-ended operatives (i.e., their mission does not include their safe return) who share a common ideology and cultural bonds that are the basis of an elite and committed 4GW force. How does our police operations compare to this formidable clandestine para-military force in the homeland ? We will need to examine this question on several fronts including police training, resources/funding, technology and crime analysis.

Police Training and Preparedness

Looking at the breakdown of the types of police training and preparedness is a critical task in evaluating how effective police operations are at handling 4GW attacks. In the resource of Federal Support for Local Law Enforcement (21), a review of Federal funding and training shows that "between FY2009 and FY2014, the federal government provided nearly $18 billion dollars in funds and resources to support programs that provide equipment and tactical resources to state and local LEAs." Since 9/11, the Congress and Executive Branch have been steadily increasing aid to LEAs (Law Enforcement Associations) due to the growing threat from 4GW activities, shrinking local budgets and the ease of accessibility that violent criminals have with respect to military-capable weaponry. However, most of the support is in the form of non-controlled equipment like office furniture, computers and other technological equipment, personal protective equipment and basic firearms. Controlled equipment with 4GW capability is only funded to the tune of 4% of the funds that are transferred—yet, no functional training on this equipment is provided by any part of the funding allocations by the supporting institutions! Instead, the balance of the training support is primarily focused on the areas of community engagement, oversight, training in improving general policing practices and the community policing model. Likewise, the same report shows that many of the funding administrators fear that 4GW training "may unintentionally incentivize the use of military-like tactics and equipment when unnecessary " !! So while billions of funding dollars are spent on 4GW countermeasures and equipment– there is not the same level of training funding that is necessary to operate the small amounts of controlled equipment available to the LEA's !! As we will see, this scenario is not in the best interests of the LEA's, nor the country, to help fight domestic 4GW protocols.

Resources and Funding

In addition, according to the same federal report, what non-equipment 4GW training is provided to the LEAs takes the form of continuity planning, disaster recovery and emergency management. Yet this type of funding support for police operations only covers reactive responses to 4GW attacks – it does not cover any training for inderdictive and preventative measures to 4GW attacks. This is a critical mistake in resource planning for the federal assistance to the LEAs - since the single –ended 4GW attacks are designed to drain police resources and service while future attacks are being planned and strategized. By simply funding primarily the reactive modes and training of police operations, federal support is playing into the strengths of the hostile 4GW forces. This allows successful 4GW attacks to be used for further propaganda and recruitment of a pool of operatives and agents by the hostile forces.

Technology and Crime Analysis

What is clear from the Fed Report is that there is little direct funding and support for interdiction technologies with appropriate training for Police Operations in 4GW. These technologies are available and are a reliable tools for preventative domestic operations in the 4GW realm. The learning curve for these tools is critical and law enforcement is already behind in dealing with 4GW attacks. At a conference on July 21, 2015, FBI Director James Comey indicated that for the first time the FBI is carrying out on-going terrorist investigations in all 50 states of the country. At the same time, "over 60" Islamic State plots so far this year have been investigated, according to the chair of the House Homeland Security Committee Michael McCaul. The trend for 4GW attacks is clearly growing and will threaten to overwhelm federal security agencies like the FBI. At a July13, 2016 Congressional Hearing, Mr. Comey indicated that there are "hundreds" of civilians who are vulnerable to 4GW propaganda and thus prone to carrying out violent attacks across the nation. Mr. Comey went on to say that having the FBI by itself find these potential operatives is like "finding the needle in the haystack". Local Police Operations are a key factor in taking up the slack in 4GW interdiction and therefore their targeted training in these areas needs to be underway as soon as possible.

In addition, threat/risk studies (G.G. Brown (22)) have shown the imminent vulnerability to 4GW attack in key areas of domestic operations which are so critical that any compromising of these resources would have wide-ranging impact on core qualities of stability in domestic civilization. These key areas are food and water supplies, transportation infrastructure, communication infrastructure and power and energy infrastructures. Furthermore, there are 4GW attack scenarios that show that these sensitive areas could be easily compromised through conventional weapons attacks as well as using chemical, biological and tactical radioactive weapons (dirty bombs) that would completely devastate the recovery and use of core resources for a time scale that could last 100 to 150 years (Dept HS(23)).

Technology Applications for Domestic Interdiction of 4GW actions.

All the technologies that can be used in support of 4GW interdiction approaches are primarily derived from **two fundamental techniques: real time surveillance systems and database operations with predictive analysis**. There is a **3rd human component** which will be discussed in the next section. These technologies can assist the FBI and local law enforcement with looking for the "needle in the haystack" 4GW activity that is becoming more prevalent. While no approach is perfect, these technologies can be the proverbial magnet that can be used to significantly increase the probably of successful interdiction.

Real time surveillance covers a wide range of applications and is very adaptable to a broad situational usage. The issue of surveillance is generally thought of as high speed and intermittent digital video and image capture applications. Yet in reality, surveillance goes beyond this classic understanding and is re-engineered to cover all forms of networked communications, signal capture and data storage. Futhermore, the National Commission (24) has shown that terrorist groups like Al Qaeda and others have a history of showing a preference for attacks that have different geographical sites yet have multiple and simultaneous timing. Examples of this hostile behavior include the 9/11 attacks, the African embassy bombings and the Madrid and London transportation bombings. Detailed analysis of these attacks showed an interesting phenomenon called Hostile Preoperational Surveillance (Diamond, J. (25)) which appeared as a long term, strategic procedure by hostile operatives—including a practice run several weeks before the actual attack in London.Similarly, there two practice runs made by hostile operative Mohamed Lahouaiej in the terrorist attack via 20 ton truck during the Bastille Day celebration in Nice, France on July 15, 2016. Hostile preop surveillance can also be temporal in nature, like that found by the FBI (Joint DHS/FBI Advisory (26)) in casing reports of large financial institutions which showed enhanced activities on Wednesdays. These isolated events on their own may not reveal a pattern or designated plan, but taken collectively via Defensive Recon Surveillance, this information can form the basis of interdictive deployment of Police Operations that increases the likelihood that law enforcement personnel will be able to intercept the hostile agents before any attack can occur and/or assure police resources will be in place when and where the hostile behavior is likely to occur.

To use any real time surveillance information in a meaningful actionable manner, a high speed database system must be employed to "data mine" any significant hostile and criminal activity predictions. This is the second item in the triad of interdictivetechnologies. . Database operations and predictive analysis of hostile or criminal activity is a growing area of law enforcement tools that are being brought to bear on interdiction with much success. Database Operations (DO) are frequently combined with Geographical Information Systems (GIS) to produce a powerful analysis and prediction tool that has been shown to do accurate crime and hostile activity forecasting. Normally, this combined tool system works with overt crime data which is readily available from police operations reports. In the case of 4GW hostile actions, data can come from several overlapping sources, domestic and foreign, causing a wide range of scattered data which realistically can only be analyzed by digital DO systems. In these cases a baseline of suspicious hostile behavior can be established which forms the foundation for making predictive estimates in time, location and personnel typically involved with such actions. This type of forecasting accurately places police and law enforcement resources in the best arrangements to deploy, interdict, mitigate and apprehend hostile 4GW agents and operatives before the loss of life or destruction of infrastructure. Training police and law enforcement agents in the use of these tools is critical-- especially in cases where short time frames may be in play and results are needed in the field in an imminent situation.In the right configuration, DO/GIS systems can produce high accuracy and have produced successful interdiction in a majority of the applications (National Institute of Justice(27)).

Another important aspect of DO/GIS systems is the creation of "fusion centers" that create integrated predictive analysis by interconnecting or "fusing" local, regional and global data "warehouses" that can store and retrieve 4GW information and data in real time and allow "just-in-time" analysis support for law enforcement operations on site. Using special modes called unsupervised learning algorithms, automated programs using clustering techniques can use fused data to quickly identify and uncover obscure and unknown patterns of hostile origin and development.Using this approach will avoid the use of generic Profiling techniques which has become rather controversial in its applications of Police ops. Training for police operations and full implementation of these4GW technologies needs further funding and support to reach complete operational status.

4GW Human Resource Support for Police Operations

There are several approaches in personnel and human resources support that can be used to meet the rising impact of 4GW on Police Operations. These proposals require the reorganization of law enforcement divisions into hybrid departments that are better suited to meet the shift in 4GW actions. These areas are Natural Surveillance, Infiltration, Civil Intell Bureau and Domestic Special Forces.

Natural Surveillance

In many hostile actions and criminal incidents, it is not unusual to have witnesses in debriefings to detail previously unreported suspicious behavior that was a portend of imminent events.If these events could be reported as unusual or pre-incident behavior, where investigations could show linked and connected suspects, then a high level of interdiction can take place. This type of approach has been outlined by De Becker (28) in the late 90’s with case histories concerning reported workplace violence data from witness information This approach is called Natural Surveillance (NS) and its goal is to take compiled data from past police reports, civilian witnesses, public records, local civil patrols, etc,,,,, that can be used to directly and timely for actionable operational interdiction.A recent example of NS is the hostile ambush and killing of 3 police officers and critical injury to 3 additional officers in Baton Rouge, Louisiana on July 17, 2016 by Gavin Long. Earlier in the day of the attack, witnesses reported seeing two men changing into dark clothes in a building nearby the site of the attack. In addition, two weeks earlier, an incident of a nearby pawn shop break-in took place where the captured perpetrators stole guns and ammo to be used to “kill cops” as they told they police investigators. Unfortunately, these NS data reports were not incorporated into any data mining investigations.

There are very significant and direct benefits from using this approach: a) most importantly, NS provides orders of magnitude increase in the generation of reliable investigative data that law enforcement agencies and national agencies like the FBI would need to find the hostile agent, hostile operation, criminal activity or “needle in the haystack” as described by Director Comey. b) deploying operational personnel basedon NS can lead to further observations and confirmation of the reported illicit behavior, and to provide a quick response in the case of any escalation, c) deterrence of any suspicious or unusual behavior by deployed personnel, d) NS targeted deployment provides a visible presence based on public input and feedback which can enhance a perception of increased public safety in a given location.

One aspect of NS that will occur is the generation of high volumes of data from public input streams – but this is an effect that is perfectly matched for the “data warehouses” and high speed computer-based data mining systems mentioned in the previous section. Current funding and training for NS and data mining operations is not yet at sufficient levels to make these valuable techniques viable for police and law enforcement operations (Markle Foundation (29)).

Law Enforcement Intelligence Bureau

On December 4th, 1981, President Ronald Reagan created the United States Intelligence Community by executive order. The United States Intelligence Community(I.C.) is a federation of 16 separate United States governmentagencies that work separately and together to conductintelligenceactivities considered necessary for the conduct offoreign relationsandnational security of the United States.In addition, there are 4 more federal agencies that were designed to share and interconnect all the intelligencedata that is generated by the IC. However, the IC and its 20 agencies has become a top-heavy bureaucracy that cannot collect and dispense operational intelligence in an actionable manner that can be applied to timely domestic interdiction. Part of the problem is that portions of the data are classified and cannot be distributed – but the IC is not designed to be local in nature and it does not usually interact directly with local or regional police and law enforcement operations in a timely interdictive manner.

What is needed to fill the gap of intelligence data information for police operations is the creation of a targeted bureau that can be a domestic fusion center that is focused on 4GW interdiction operations for local police operations across the nation. The author of this paper is proposing that there is a critical need for a new bureau to be formed as a dedicated agency that serves all intelligence needs and analysis of the law enforcement and police agencies. While there exists a Law Enforcement Partners Board within the Dept of Homeland Security, it exists mainly as an advisory body for the Director of National Intelligence.

There also exists a member-driven associationknown as Law Enforcement Intelligence Units (LEIU) that has more than 240 members of domestic police and law and enforcement agencies who have common interests in sharing intelligence data among their member agencies. While this association is not a formal, government funded agency, it would be a very appropriate model to create the basis of just such a certified government bureau, with a focus on 4GW data collection and analysis from all domestic agencies, including NS records and related information to be used in imminent interdiction police operations. As we have seen, a new Law Enforcement Intelligence Bureau is an agency that is critically in demand nationally to fill the immediate interdiction intelligence needs of police operations who are in desperate need of training and funding for implementation of current analysis technologies reviewed in this paper.

4GW Counter Infiltration

A final component of the human resource support for countering 4GW action is Counter Infiltration Operations (CIO) carried out by law enforcement personnel. This concept has become a necessary tool to supplement an overall defense-in-depth approach to counter 4GW hostile actions in the homeland. CIO has an extended history of application in domestic criminal justice investigations of organized crime operations dating back 80 years in the U.S. In the early periods of it use, CIO was launched to investigate the corruption and influence of organized crime infiltration on local police officials, judges, court administrators, politicians, etc….At that time, corruption was so rampant in local and in some federal jurisdictions, that special CIO squads were formed by hand-picked law enforcemtn personnel that were so committed to their anti-crime mandate that they were labeled "untouchable". In today's environment, corruption is a lesser issue then before and forming untouchable squads is rather easy. However, the current environment of 4GW actions is complicated by terrorist and gang-related activity that is frequently associated with religious fundamentalism and/or cultural and ethnic influences and beliefs that are intertwined within the areas of certain civilian populations. 4GW CIO carried out in these applications requies a certain level of profiling and cultural training for targeted communities. In some political arenas, this may cause the CIO operations to be labeled as controversial and their implementation to be called into question. To negate this situation, crime statistics and data analysis must be brought into play so that complete objectivity forms the basis of the operations—regardless of the religious and ethnic factors involved in the original 4GW or criminal activity. There are two basic forms of CIO that can be applied to 4GW actions: covert infiltration and cognitive infiltration.

Covert Infiltration

This type of infiltration involves one or more police agents taking on alternate identities and backgrounds to slowly penetrate suspected or known domains of gangs, organized crime or terrorist cells. This process is very strategic in nature, i.e., evolving into a mature and accepted "plant" of a law enforcement agent over a long term and wide range. As a result there can be a significant investment in time and effort before any useful information can be generated for effective police interdiction. Ideally, the police agent should be socially "untouchable" so that he or she does not have family ties or social obligations that would be a detriment to the overall covert operation. The agent also assumes a risk of discovery and hostile retaliation in any encounters with hostile operatives that may initially develop at the beginning of the operation. One advantage of this type of operation is that the alternate identities can easily be arranged through official supporting government offices that keep records of "official" citizen identities. Once established, a successful Covert Infiltration (CoIn) can produce many significant benefits to life-saving interdiction operations. In the case of domestic terrorist cells, the implementation of CoIn is easier to establish because many cells rely on deep cover operations where they are isolated from communications and contacts with other hostile operatives – thereby allowing police operatives ample time to establish trusted connections to terror suspects through cultural and ethnic backgrounds without arousing suspicion from other cell members. There are two legal hurdles involvingCoIn that may become real issues if not handled properly. These legal aspects are 4th Amendment violations and entrapment. In the first case it is imperative that the police agent's supervisor have any and all confidential search warrants in place before any covert infiltration begins. In the second case, the police agent must be careful not to initiate any illegal activity that leads hostile contacts to expand the nature and range of the illicit activity—otherwise any evidence generated in this manner may not be admissible in court. Lastly, the police agent may have to be trained to interdict with deadly force in the course of the covert infiltration if other citizen's lives have become exposed to immediate andimminent danger. The final decision in this case may be up to the police agent alone who has free license due to the covert nature of the operation.

Cognitive Infiltration

In this category of infiltration, there are two sub classes to consider. In the first class, Cognitive Infiltration (CogIn1) deals with finding the sources of 4GW propaganda and initiatives through direct contact or via social communications systems (Facebook, Twitter, Blogs, etc…) by posing as a potential new member of a gang or terrorist cell. In this case, the goal is not to physically infiltrate the hostile force, but to simply ID leaders or the upper echelon of the hostile organization while gathering information about their activities.This class of infiltration could lead to deeper involvement as needed depending on the specifics of the 4GW activity, possibly leading to a fully developed Covert Infiltration plan.

In the second class category, Cognitive Infiltration (CogIn2) includes the involvement of 4GW Conspiracy Theories. In these situations, law enforcement activity is concerned with violent behavior from hostile gangs or terrorist cells that have been strongly influenced by propaganda deliberately based on overlapping phases of faulty information. This theory was first formulated by Sunstein and Vermeule (30) where they identified the negative effect of conspiracy theories on the ability of government and law enforcement to carry out anti-4GW policies in critical hostile actions. As an example, they pinpoint the groups that promote the view that the US Government was responsible for, or complicit in, the September 11 attacks as "extremist groups." To counter this effect, they proposed that "the best response consists in cognitive infiltration of extremist groups",where they describe this class of infiltration as, "Government agents (and their allies) might enter chat rooms, online social networks, or even real-space groups and attempt to undermine percolating conspiracy theories by raising doubts about their factual premises, causal logic or implications for political action." Even as some criminal justice scholars do not ascribe to their conspiracy theory, (CogIn2) is a legitimate response to 4GW actions related to gang violence and terror cells since it can be a powerful interdiction tool regardless of whether conspiracy initiated the action or not. Indeed, many criminal justice researchers (Zager and Zager(31)) see (CogIn2) as one of the most effective 4GW countermeasures since it directly addresses the impact that today's digital social media has on public awareness of law enforcement operations and policies.

However, (CogIn2) can also have some vulnerabilities in terms of its use by law enforcement. Unless (CogIn2) is carried out as a total covert action, its use may create a tradeoff between credibility and control. Stated another way, the price of credibility is that law enforcement cannot be seen to control public opinion and independent thought. This position has been supported by some legal academic researchers who argue and critique that it would violate prohibitions on law enforcement propaganda aimed at domestic citizens (Hagen(32)). So using (CogIn2) in this manner could require confidential proxies be in place before this approach is initiated.

In an ironic twist, it should be well noted here that (CogIn2) is also an effective tool for 4GW operatives in support of their strategic hostile actions. Many researchers have shown that the radicalization of foreign nationals and naturalized citizens takes place through an extended and relentless onslaught of (CogIn2) propaganda streams. *Indeed, this approach is at the very heart of the 4GW attack protocols !* Furthermore, it has been shown (B Leclerc, R Wortley(32)) that domestic movements, politically extreme groups and gang related activity all make extensive use of (CogIn2) in one form or another – e.g., Occupy Wall Street, MoveOn.org, BlackLivesMatter, etc… In addition, the recent ambush attacks on police forces in Dallas, Louisiana, and Milwalkee had perpetrators who aggressively repeated the propaganda and reasoning for their ambushes that mimicked and paralleled similar talking points from the associated movements' websites, blogs and pod casts.

So we have the case where (CogIn2) is being used extensively by 4GW operatives from terrorists as well as domestic insurgents and gangs and resulting in successful 4GW violence in domestic incidents. The question is whether law enforcement should respond with their own (CogIn2) counter measures. The answer can be reached by doing a risk/threat assessment of that approach in each application. In most cases, the threat involves public discovery and exposure of the law enforcement infiltration technique as a covert operation which may have a negative perception by the public-at-large as a government intrusion and/or interference into the private cyberdomain of citizens. However, the risk level of this threat can be lowered significantly if the counter (CogIn2) activity by law enforcement personnel is carried out independent of any police or law enforcement "official" policies or duties—e.g., it is carried out as private citizens who are not "on the clock" and are simply exercising their own 1st Amendment rights. Once the countermeasures are put into place, other law enforcement personnel can then resume their official surveillance and monitoring of the status of any continuing 4GW activities that may react/interact to the active countermeasures.

Summary & Conclusion

Summarizing our previous discussions, the 4th generation of warfare as identified by theoretical analysis of military evolution is a new phase of enemy strategy that bypasses the previous levels of armed forces and weapons defenses and brings the battlefront squarely into the domain of police operations and local law enforcement. This new type of military aggression clearly is substantiated by the growing hostile homeland attacks that have been taking place globally over the last two decades. In addition, this new evolution of warfare tactics has also "bled" into the domestic criminal elements like gangs and related movements that have been using them against police operations with great regularity and with unexpected success. This places a great burden upon police and law enforcement operations which must now be prepared to handle both hostile forces acting domestically as well as domestic criminal elements using the same para-military warfare tactics to carry out their criminal activities and to promote radical ideologies.

It has been shown that police operations are not fully prepared to meet this double threat posed by 4GW. Government support and resource allocation for law enforcement is not focused on the internecine nature of 4GW, but is rather limited to the reactive post-attack emergency response approach which only emboldens the 4GW hostile actors to increase their scope and range of attacks. The latest military-style interdictive support, training and deployment must be brought to bear in the realm of police operations to stem the wave of 4GW hostilities. Several areas of application have been identified in this paper as lacking in the police operational readiness to 4GW. These areas include technologies like real time surveillance systems and database operations with predictive analysis, data mining and fusion centers. On the human resource and training side, other approaches like natural surveillance, 4GW infiltration techniques, civil intelligence bureaus and law enforcement intelligence bureaus need to be established. All aspects of this interdictive approach to updated law enforcement operations for 4GW hostilities can be brought together in a new Domestic Special Defense Forces Operations. This arrangement will help to centrally deploy technology and training to targeted and highly susceptible areas of domestic police operations across any given national government.

References

1. Lind, William S. "Understanding Fourth Generation Warfare." ANTIWAR.COM 15 JAN 2004 29 Mar 2009
2. Colonel Thomas X. Hammes, 'Four Generations of Warfare' inThe Sling and The Stone: On War in the 21st Century, St. Paul, MN. 2006, p 29
3. Echevarria JA.Fourth Generation War and Other Myths.November 2005, Strategic Studies Insititute.
4. Thornton, Rod (2007).Asymmetric Warfare. Malden, MA: Polity Press
5. Beyond Fourth Generation Warfare, Dr. George Friedman, Stratfor Forecasting, p. 1, July 17, 2007
6. Schmitt, John F." Command and (Out of) Control The Military Implications of Complexity Theory", 2004.
7. Arquilla, J., Ronfeldt, D, and Zanini, M."Networks, netwar and information-age terrorism", RAND Corporation, 1999
8. Ghanshyam. S. Katoch, Fourth Generation War: Paradigm For Change, (June, 2005). Masters Thesis submitted at The Naval Postgraduate School, Monterey, California. Available from Defence Technical Information centre at www.dtic.mil/
9. Richard Cohen Pittsburgh Post-Gazette - May 27, 1988 "Soviets can't blame their liberals for Afganistan"
10. Papyrus News, 2002, Fourth Generation Wars; Bin Laden lieutenant admits to September 11 and explains Al-Qa'ida's combat doctrine. Februrary 10th, https://mailists.uci.edu/mailman/listinfo/papyrus-news.
11. Wall Street Journal, January 7, 2015, "Timeline of terror attacks over the last 20 years."
12. WSJ, Nov 14, 2015, Timeline: Terror Attacks Linked to Islamists Since 9/11 - WSJ.com
13. J Washington Times ,June 21 2016 Reconsidering safe zones in Syria -
14. The Washington Post ,The diplomatic case for America to create a safe zone in Syria - The ... https://www.washingtonpost.com/...safe-zone-in-syria/.../f3c7c820-... Feb 4, 2016.
15. World Politics Review , The Powell Doctrine's Enduring Relevance - World Politics Review www.worldpoliticsreview.com/articles/4100/the-powell-doctrines-enduring-relevance Jul 22, 2009
16. Back to the Weinberger-Powell Doctrine? - U.S. Air Forcewww.au.af.mil/au/ssq/2007/Fall/Record.pdf Strategic Studies Quarterly ♦ Fall 2007 United States Department of the Air Force by J Record - 2007 - Weinberger-Powell Doctrine? Jeffrey Record
17. James E. Armstrong III, MAJ, From Theory to Practice: The Powell Doctrine, 2010, U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301.

18. Los Angeles Times ,Deadliest U.S. mass shootings, 1984-2016 - Timelines - Los Angeles ... timelines.latimes.com/deadliest-shooting-rampages

19. Medical News Today ,Gang Membership Tied To Mental Health Problems - Medical News ... www.medicalnewstoday.com/articles/263279.php Jul 12, 2013 –

20. Washington Times, Majority of fatal attacks on US soil carried out by ... - www.washingtontimes.com/.../majority-of-fatal-attacks-on-us-...The Washington Times Jun 24, 2015

21. Review: Federal Support for Local Law Enforcement Equipment Acquisition; Executive Office of the President December 2014, https://www.whitehouse.gov/.../federal_support_for_local_law_enforcem

22. GG Brown , Analyzing the Vulnerability of Critical Infrastructure to Attack and ... faculty.nps.edu/.../DefendingCIBrownEtAlTutorialDraft.pd Naval Postgraduate School .

23. DHS, Communicating in a Crisis: Radiological Attack - Homeland Security https://www.dhs.gov/.../prep_radiolog..

24. 9/11 Report - National Commission on Terrorist Attacks Upon the… www.911commission.gov/report/911Report_Exec.htm

25. Diamond. J. (2006), Insurgents give US valuable training tool. USA Today, January 2006.

26. Joint DHS and FBI Advisory Title: Homeland Security Advisory System Increased to ORANGE for Financial Institutions in Specific Geographical Areas Date: August 1, 2004

27. National Institute of Justice ,Predictive Policing: The Future of Law Enforcement? | National ... www.nij.gov/journals/266/pages/predictive.aspx National Institute of Justice Jun 23, 2010 - Law enforcement explores ways to anticipate and prevent crime. .. November 2009.

28. DeBecker, G. 1997, The gift of fear. Little, Brown and Co., New York

29. Markle Task Force on National Security in the Information Age, with James Steinberg, VP and Director, Foreign Policy Studies (2002), Protecting America’s Freedom in the information Age.

30. Sunstein, Cass R.; Vermeule, Adrian (June 2009). "Conspiracy theories: Causes and cures". Journal of Political Philosophy. Wiley. 17 (2): 202–227

31. R Zager, J Zager ,Deploying Deception Countermeasures in Spearphishing Defense - researchgate.net

32. Kurtis Hagen, “Conspiracy Theories and Stylized Facts,”Journal for Peace and Justice Studies 21.2 (Fall 2011) 3–22.

33. B Leclerc, R Wortley , Cognition and crime: Offender decision making and script analyses, Springer Intl. Pub.. – 2014.