National Intelligence Estimate

The Outlook for Intelligence Collection

Fuad Guliyev

George Washington University,
Washington DC, USA

KEY JUDGEMENTS

US Intelligence Community faces qualitatively new environment after the Cold War when older means of intelligence gathering is challenged by Fourth Generation Warfare techniques that can't be countered in traditional way.

- Although there is no longer such an overwhelming threat like Warsaw Pact, there are new threats to US national security such as international terrorism, organized crime, drugs and human trafficking, illegal arms trade and increased threat of WMD proliferation. Traditional intelligence collection methods prove to be difficult to face this new challenge some of which can be further elaborated to be part of so called 4th generation warfare.
- Certain nation-states such as China and Russia still require attention from intelligence community. The list can be even extended to rogue states such as Iran, Syria, North Korea or Sudan. Even allied and partner countries may require attention too as Indian nuclear test of 1998 proves that. This fact emphasizes continued need for more advanced space-based intelligence gathering platforms.

9/11 terrorist attacks surfaced the weaknesses within US national security system. As Congressional investigation shows there is a need for a better partnership between various security agencies that so far have been reluctant to work together. This NIE proposes three possible scenarios of such partnership.

- Total integration of US national security system under single federal agency. This is the least likely scenario given the political culture of United States and history of relationship between involved agencies.

- Cooperation model is reserving more powers to newly established Director of National Intelligence. It would mean decrease in authority of individual agencies. Therefore this scenario also enjoys less chance of probability.
- Collaboration model envisages individual agencies still retaining to their traditional powers but doing more information sharing and coordination under DNI. According to this NIE this last scenario is the most likely one.

The problems faced by US post-Cold War intelligence community can be classified into two categories, being organizational, as discussed above, and technological. Despite the significant technological superiority enjoyed during the Cold-War, evolved circumstances make development of new technologies necessary to tackle old problems and to counter the qualitatively novel challenges. Arrival of Fourth Generation Warfare means traditional intelligence collection methods are either mostly irrelevant or hard to exploit because rival usually employs low-level technology and pays more attention to denial and deception. According to NIE changed face of warfare may force US intelligence community to choose one of the three possible scenarios:

- Employing revolutionary ISR platforms, such as Future Imagery Architecture, to meet the new challenges by increased reliance on even higher level of technology. It would be a forward-looking strategic initiative which is not likely to happen because development of such systems will require multi-billion investments that hardly will be approved by Congress, even in post 9/11 environment.
- Second scenario is shifting back to legacy systems as modern rivals make it hard to collect intelligence by sophisticated ISR platforms due to adversaries' preference of lower level technology to deny information to the opponent. Return to legacy systems seems to be the least likely scenario.
- The most likely scenario is US intelligence community will opt for mixture of the tactical and strategic intelligence collection methods. It will depend on the specific circumstances and decision will be made on case by case basis. It is about balancing strategic priorities versus tactical needs. At both levels there is still a growing need for more advanced space-born technologies.

DISCUSSION

Congressional investigation of 9/11 terrorist attacks revealed that actually there was some information available about possible attacks. These warnings even kept

rising since late 90s until summer 2001[1]. Informants within Al-Qaida even warned about possible attacks to World Trade Center or employing planes as missiles. Intelligence community was also informed about several terrorism suspects' arrival to the country. Still terror act was not been prevented.

When asked why one can arrive to a "wheat and chaff" dilemma which is a daily problem in intelligence community, meaning valuable information is so fragmented and spread out across such a broad spectrum that it is impossible to bring the pieces together and analyze them. Although intelligence analysis is not the area of concern to current NIE lack of imagination for analysts' part certainly played a destructive role too. Although intelligence community did react to the warnings, analysts were not creative enough to imagine possibility of attack directly to continental US[2]. Better intelligence collection techniques might have compensated for analytical failure.

One example to that is interception of communications between Al-Qaida members. Although some information traffic was detected as a general rule plotters observed a strict silence which made signals intelligence almost irrelevant. Even acquired pieces of information usually looked odd in the background of volume of communications being analyzed. More advanced software to track the communications traffic might have helped to concentrate on more important pieces of information lost in vast amount of data.

Poor human intelligence, such as small number of informants within Al-Qaida and their questionable loyalty also added to the problem excluding possibility of HUMINT correcting shortcomings of SIGINT. But analytical deficiency was further exaggerated by non-cooperation between individual security agencies. Ideally different fields of intelligence should work together towards common target[3]. It is necessary because all the individual branches of intelligence gathering have own disadvantages. So the best decisions are made based on information gathered from as many sources as possible. However CIA, FBI and NSA all having access to pieces of valuable information failed to cooperate to prevent surprise attack. Have they shared the information available to them with one another there would be a more detailed picture which would help the analysts.

[1] Senate and House Joint Inquiry Statement on the 9/11 Terrorist Attacks, pg 7
http://www.gpoaccess.gov/serialset/creports/pdf/fullreport_errata.pdf
[2] Ibid pg 8
[3] Lowenthal, Mark M. Intelligence: From Secrets to Policy (Fourth Edition). CQ Press. Washington DC 2005 (Paperback) 2009 pg 71

For all these reasons 9/11 terror attacks are not the result of simply analytical failure, it would be fair to suggest that they took place more because there were organizational and technological problems in US intelligence community that went unnoticed in post-Cold War era.

Despite of the fact that Warsaw Pact doesn't exist anymore national security environment for United States became even more complicated. While countries with nuclear arsenals like Russia and China still require attention others like North Korea and Iran try to develop ICBMs of their own. Even allied and partner countries such as Israel, India and Pakistan may require attention as India's surprise nuclear test of 1998 proves it[4].

However the most striking feature of post-Cold War era is increase of threat by non-state actors like terrorists and organized crime. As 9/11 events and military operations in Iraq and Afghanistan teach it is these non-traditional rivals that pose more serious threat to US national security. What makes these groups so dangerous is that they are employing 4th generation warfare techniques.

Although this NIE is not a supposed to be a military research paper it would be useful briefly to touch the issue of warfare generations as it affects so heavily the way how intelligence is collected nowadays. It is believed that warfare techniques went through three generations. The first generation is the time when militaries used muskets and soldiers lined up to maximize the fire power[5]. Both technological factors and social conditions shaped each generation. Second generation was marked with introduction of indirect fire and rapid movement. Mass firepower replaced importance of mass manpower, this was the primary difference[6]. Third generation warfare was heavily dictated by ideas and immediate needs, realities rather than technologies. The concept of *Blitzkrieg* that was developed by Germany already by the end of 1918 is a good example of ideas driven warfare[7]. Each generation was different from previous one in terms of even wider projection of power.

Analysis of conflicts after WW II show that the next generation is likely to be highly technology driven and encompass entire society of the adversary[8]. High-

[4] George, Roger Z and Bruce, James B Analyzing Intelligence Georgetown University Press. 2008

[5] Lind, William S. and Col. Keith Nightengale, USA, Capt. John F Schmitt, USMC, Col. Joseph W.Sutton, USA, and LtCol. Gary I Wilson, USMC. "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette*, Oct 1989 pg 23

[6] Ibid

[7] Ibid

[8] Ibid pg 24

tech nature of 4th generation warfare is manifested in current "smart bombs" or space-enhanced military operations. However it is likely to go even further by militaries concentrating on electronic and cyber attacks or jamming the adversary's telecommunications satellites to paralyze its force. Prospect of more advanced technologies and efficient military systems such as space based weapons will reduce the number of combatants involved in the conflict. Future militaries will be more about technically high skilled professionals that will be more flexible and mobile than contemporary armed forces. Quality will overwhelm quantity. No wonder that amount of C3D2 employed by rivals will increase significantly by as early as 2015[9].

4th generation warfare also affects the entire society of the adversary trying to degrade the social, economic and military infrastructure. It is about winning the minds of adversary and neutral or allied international community. So it would be correct to conclude that fourth generation war is also an information warfare. It is about changing the opinion how adversary, allies and neutrals think about the war and themselves in general. Information warfare is not just about reaching one's message to the audience but is also about persuading the opposition that conflict can't be won militarily. High-tech nature of modern warfare is not just manifested in "smart" bombs it is also about skills to use means of multimedia in one's own advantage.

As recent developments show 4th generation has technological and social aspect. Depending how advanced the adversary is it can emphasize the former or latter aspect. While anti-satellite missile test of China stresses the technological aspect, terrorist attacks of 9/11 or suicide bombs in Middle East are examples of technologically inferior adversary trying to achieve political means by information warfare, by spreading the message and targeting the entire society. Moreover unlike traditional militaries terrorists of 9/11 and insurgents in Middle East deliberately avoided intense communications or fixed headquarters and camps to deny intelligence collection. Although weaker in terms of force tactics employed by insurgents in Afghanistan and Iraq may prove to be more dangerous if exploited by more advanced militaries such as that of China, Russia or India.

US intelligence community was not prepared enough neither technologically, nor organizationally to face this new type of challenge. The most destructive reality was existence of competition and stovepipes- distinction of intelligence agencies based on technical and non-technical collection methods. Usually any given intelligence branch is constrained by certain other factors too, such as budget,

[9] Diamond John M. "Re-examining Problems and Prospects in US Imagery Intelligence" pg. 61

limited number of ISR satellites, competing priorities, need to protect the source of information and identifying the most relevant information among the stream of data[10]. Among these factors prioritization is becoming more and more visible issue. It expresses itself as tactical needs versus strategic objectives. Intelligence collection serves both long-term and short-term needs. While Cold War period more stressed the need for strategic planning and intelligence gathering that aimed at that, current landscape is not about global political competition between two superpowers. Short-term regional armed conflicts make tactical needs of military more pressing issue. But on the other hand nation-states like Iran carrying out underground nuclear research reminds that strategic intelligence gathering is still important. Both levels require technological improvements. This NIE finds it useful to zoom more in depth into different intelligence collection disciplines to have a broader idea what they are expected to do and what the problems are that they face.

HUMINT or human intelligence is usually about sending trained intelligence officers to the denied areas, as in case of H.K. Roy in Sarajevo[11]. His mission was to collect information but in most cases HUMINT is more about appointing some intelligence chiefs in country of interest who would then recruit informants among locals. It is the informants who usually do the actual espionage. Usually appointing intelligence officers abroad involves inventing pseudo names and cover stories to give them a plausible reason for living in the area of interest. It is easier if intelligence officers enter the country under the cover of diplomatic activity, such as chief officer Hathaway who was the case officer for the Tolkachev[12]. But such operations may cause controversy if the officer is intercepted by the counter-intelligence of host country.

As Cold-War experience in West Germany shows open nature of democratic societies make it easier for adversaries like Stasi to recruit assets of their own by exploiting the basic human weaknesses of even staunch anti-communists like Hans Rehner[13]. Need for more effective counter-intelligence and intelligence network within hard to penetrate targets like terrorist groups calls for more attention to

[10] Lowenthal, Mark M. Intelligence: From Secrets to Policy (Fourth Edition). CQ Press. Washington DC 2005 (Paperback) 2009 pg 53

[11] Roy H.K, "Betrayal in the Balkans" Intelligencer: Journal of US Intelligence Studies, Volume 12, No 1 (Summer 2001) pg 45

[12] Royden, Barry G., "Tolkachev, A Noteworthy Successor to Penkovsky," Studies in Intelligence, Vol.47 No 3 (2003)

[13] Macrakis Kristie, "The Case of Agent Gorbachev", Intelligencer: The Journal of US Intelligence Studies, Vol. 12 No 1 (Summer 2001) pg 11

HUMINT. Traditionally CIA was in charge of clandestine HUMINT operations overseas, whereas FBI more concentrating on domestic counter-intelligence.

TECHINT is the term referring to technical intelligence collection disciplines that further break down to SIGINT (signals intelligence), IMINT (images intelligence) and MASINT (measurement and signature intelligence).

The primary security organization in charge of SIGINT in United States is the National Security Agency. Usually intercepted signals are about two-way communications. That is why COMINT- communications intelligence is considered to be part to SIGINT. Signals intelligence is a struggle between cryptographers and counter-intelligence encoders that try to code the communications signals to prevent interception[14]. TELINT- telemetry intelligence and ELINT-electronic intelligence are also sub-branches of signals intelligence and helpful to analyze the weapons testing or picking the ranges of frequencies that enemy uses. Disclosures of most United States SIGINT capabilities made denial and deception techniques of adversaries even more sophisticated. There is a need for more advanced systems on ground and space-born platforms to maintain US dominance in the field. As 9/11 example proves part of the problem was NSA being overwhelmed by stream of data.

Another major technical intelligence collection discipline is imagery intelligence. IMINT is a field where US traditionally enjoyed superiority compared to rivals by initiating the CORONA program- series of spy satellites. Although IMINT is coined with the name PHOTOINT- photo intelligence, only some portion of imagery intelligence comes from electro-optical systems. IMINT is usually about exploiting radars on satellites to penetrate the clouds, the most advanced of which is SAR- synthetic aperture radar being capable of day and night multiple detailed scan of area of interest. Usually satellites concentrate on infrared bands of the electromagnetic radiation. They "see" the warm objects that radiate infrared waves. Major improvements in the field are introduction of multispectral and hyperspectral imagery that allows satellites to provide more detailed images of the targets by analyzing more than one band of spectrum[15]. Current US IMINT capabilities are provided by 5 high-resolution satellites, 3 advanced KH-11 series spy satellites and 2 Lacrosse type radar imagers[16]. NRO- National Reconnaissance Office is responsible for development and acquisition of IMINT satellites, while

[14] Lowenthal, Mark M. Intelligence: From Secrets to Policy (Fourth Edition). CQ Press. Washington DC 2005 (Paperback) 2009 pg 65
[15] Ibid pg 61
[16] Diamond John M. "Re-examining Problems and Prospects in US Imagery Intelligence" pg 62

NIMA- National Imagery and Mapping Agency is in charge of dissemination, tasking, exploiting and distribution of raw imagery provided by satellites.

Wide range of post-Cold War areas of interest, such as nation states applying more complicated denial and deception to short-term battlefield requirements call for increase in number of satellites deployed in orbit. There is also demand for qualitative change too. Shift from long-term strategic priorities to short-term tactical needs of warfighter require brand new type of satellites.

MASINT is another branch of technical intelligence that encompasses everything not covered by SIGINT or IMINT. MASINT detects, track, identifies and describes the object of interest by measuring the signature of the past activity[17]. Defense Intelligence Agency is the main security office concentrated on this field. It is debatable if MASINT an independent discipline or sub-branch of SIGINT and IMINT.

Although counter intuitive to the nature of intelligence gathering after collapse of communism open source information has grown so much that new branch of intelligence collection emerged, named OPINT- open source intelligence. It is enough to mention that 80% of the valuable information about Russia is open-source[18]. Usually high volume of information available on academic publications, mass media and internet require establishment of special research and analysis departments in charge of OPINT.

ALTERNATIVE SCENARIOS

Post 9/11 environment stressed the necessity of more cooperation between intelligence agencies. There are calls for an "integrated collection enterprise" meaning coordinated target development, collection and data management, planning, investment and development of new techniques[19]. Directorate of National Intelligence is supposed to be the overarching body that serves as the forum where all the other 16 individual agencies can do information sharing and discuss the issues on agenda. It is more of a collaboration model than integration or deeper cooperation. Current flow of events even after the 9/11, points to the fact that individual agencies are not likely to be integrated into single intelligence

[17] George Roger Z. and Kleine, Robert D. (Eds) Intelligence and National Security Strategist. Macartney, John "John, How Should We Explain MASINT?" pg 69

[18] Lowenthal, Mark M. Intelligence: From Secrets to Policy (Fourth Edition). CQ Press. Washington DC 2005 (Paperback) 2009 pg 69

[19] Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction March 2005 pg 357
http://govinfo.library.unt.edu/wmd/report/chapter7_fm.pdf

department. Powers of DNI are not so far-reaching either to allow it supervise very strong agencies such as NSA or CIA that would resist to give up their powers.

Battlefields of Iraq and Afghanistan show how enemy can avoid traditional intelligence collection methods by just preferring low-tech communications. SIGINT satellites at times fail to intercept them. IMINT is also of not much help because insurgents or international terrorism doesn't have fixed headquarters or any place where they might be bound to. Even nation states such as Iran prefer new ways of denial by moving its nuclear program deep underground.

This makes US either to shift to simpler forms of intelligence gathering such as legacy systems to "listen" to short-range radio transmissions of insurgents in Afghanistan or sophisticate current SIGINT and IMINT satellites to an extent that they can tune to low technology communications or "see" the underground targets.

As for now US intelligence community doesn't look like neither to give up operating current platforms in favor of legacy systems nor tends to revolutionize the satellites to costly levels. Current trends in technology development aim to address the pressing tactical needs at affordable rates.

Moving Target Indicator program of NRO is one of the examples[20]. MTI program is essential for warfighther because current ISR capabilities stress reconnaissance over surveillance, surveillance meaning real time observation of the objects of interest. Current IMINT satellites provide only the snapshot of the enemy troops but it takes too long to reach the friendly forces in battlefield and usually impractical if target is rapidly changing its location. Identification of moving objects is necessary for PNT- positioning, navigation and timing capability too. PNT can be further elaborated as the precision strike by space enhancement. "Smart bombs" are one example.

NRO tries not to lose the strategic grasp either. To improve efficiency commercial remote sensing is increasingly favored[21]. Even more ambitious approach was multi-billion Future Imagery Architecture program that intended develop small satellites based ISR to cut the overall costs in long run.

Another agency that amassed multi-billion projects is the NSA. In late 90s National Security Agency tried to undergo both technological and management

[20] Diamond John M. "Re-examining Problems and Prospects in US Imagery Intelligence" pg 59
[21] Ibid pg 60

reforms to improve its performance[22]. Especially there was a need for improved software to scan the communications traffic in search of important information.

As facts point US intelligence collection is neither going to shift to legacy systems to adapt low-tech nature of warfare in Middle East nor is it always favoring tactical priorities over strategic interests. It is rather mixture of both, gradually gravitating towards more advanced space-borne systems to meet the needs at strategic and tactical levels.

REFERENCES AND NOTES:

Lowenthal, Mark M. Intelligence: From Secrets to Policy (Fourth Edition). CQ Press. Washington DC 2005 (Paperback) 2009

George, Roger Z and Bruce, James B Analyzing Intelligence Georgetown University Press. 2008

Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction March 2005

http://govinfo.library.unt.edu/wmd/report/chapter7_fm.pdf

Roy H.K, "Betrayal in the Balkans" Intelligencer: Journal of US Intelligence Studies, Volume 12, No 1 (Summer 2001)

Royden, Barry G., "Tolkachev, A Noteworthy Successor to Penkovsky," Studies in Intelligence, Vol.47 No 3 (2003)

Macrakis Kristie, "The Case of Agent Gorbachev", Intelligencer: The Journal of US Intelligence Studies, Vol. 12 No 1 (Summer 2001)

Aid Matthew M. "Prometheus Embattled: A Post 9/11 Card on the National Security Agency" Intelligence And National Security, Vol. 21 No 6 (December 2006)

Diamond John M. "Re-examining Problems and Prospects in US Imagery Intelligence"

George Roger Z. and Kleine, Robert D. (Eds) Intelligence and National Security Strategist. Macartney, John "John, How Should We Explain MASINT?"

Senate and House Joint Inquiry Statement on the 9/11 Terrorist Attacks

http://www.gpoaccess.gov/serialset/creports/pdf/fullreport_errata.pdf

Lind, William S. and Col. Keith Nightengale, USA, Capt. John F Schmitt, USMC, Col. Joseph W.Sutton, USA, and LtCol. Gary I Wilson, USMC. "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette*, Oct 1989

[22] Aid Matthew M. "Prometheus Embattled: A Post 9/11 Card on the National Security Agency" Intelligence And National Security, Vol. 21 No 6 (December 2006) pg 982

Summary

National Intelligence Estimate

The Outlook for Intelligence Collection

Fuad Guliyev

George Washington University,
Washington DC, USA

The article focuses on the intelligence collection as a subfield of overall national security activity. Although main focus is on United States experience most of the conclusions it makes can be true for other countries too. One of such conclusions is that both United States and all the coalition members in Iraq and Afghanistan indeed fight Fourth Generation Warfare. Struggle against transnational terrorism is just only one manifestation of absolutely new generation of warfare. New type of warfare can be also applied by nation-states too, in this article provides the list of such rogue states purely from American perspective while realities maybe different for other countries. While new generation of war has already arrived it caught most of the countries unprepared. Article drives specific examples from 9/11 to prove how specifically intelligence collection failed in that sense.