APOJ 16-31
29 July 2016

Future Technology, Impending Security Threats

By Lt. Col. John Nolan, U.S. Army Reserve

Enormous amounts of research articles, papers and data have accumulated on the rising power of state sponsored terrorism, non-state actors, and trans-regional criminals. One can find many papers and articles that underline the role of technology. Much of the same technologies that hold the greatest promises to humanity possess the greatest concern to security if these technologies are used by maligned perpetrators. With this in mind much is being written on the distinction that can be made between a crime and what an act of war is. The purpose of this paper is to briefly and broadly discuss some of the technological advancements with the greatest potential for dual use purposes in the future. This paper also discusses the characteristics of groups or organizations the U.S. Military will most likely engage in order to shape the security environment and to carry out the *National Military Strategy 2015* to either "Disrupt, Deter and Defeat State Adversaries" or "Disrupt, Degrade and Defeat Violent Extremist Organizations."[1]

Internet, Robotics, and Biotechnology

At the forefront of technology that has delivered new capability to the global community in the form of data and information is the networked computer and the Internet. It is estimated 40 percent of households globally are connected. This is reflective of the explosive growth in interconnectivity from as recent as a decade ago.[2] It is estimated by 2020; over 50 billion devices will be connected to the Internet. Most of those devices will possess embedded microprocessors that offer real-time insights into every aspect of life on the planet.[3]

The Internet is becoming more ubiquitous in societies across the world as it becomes cheaper. Through the Internet, technological trends are shared and are accessible by cyber criminals, exploitable, and configurable to military purposes. For some context on today's commercial off-the-shelf technology capability, a second generation, game box like a Sony Play Station 2, developed in the late nineties has sufficient graphic capability to guide a missile to its target.[4]

Akin to the next generation graphics interface in a game-box, is the development of robotics technology, as commercial demand continues to grow. Research suggests that the commercial market will grow to $16.3 billion by 2020. Today's robots can perform basic motion on the ground, in the air, and in the water. Robots are able to identify objects, chart new surroundings, and perform pick and place operations. Although not entirely autonomous, robots can, to a limited extent, interact with other robots or human partners. Google, Amazon, and other companies are developing and acquiring the needed technology to build robotics, principally in the transportation sector in the form of self-driving vehicles. Major car manufacturers have announced plans to build self-driving cars and predict they will sell them to consumers by 2020.[5]

Recent studies by global industry analysts, expect annual spending worldwide on military robotics will rise from $5.6 billion in 2012 to 7.5 billion by 2018.[6] Examples of military robotics exist all over the world. The "Reaper" is the most advanced unmanned aerial vehicle or armed drone currently in U.S. inventory and deployed. China is developing their version of the "Reaper." Israel already employs unmanned armed ground vehicles, equipped with 360-degree cameras along the Gaza border.[7] The 2011 Fukushima, Japan nuclear power plant disaster has accelerated robotics with greater dexterity for going into environments where it is too dangerous for humans.

Robotics has benefited from many associated areas like data storage, computational hardware, Internet, wireless communications, electronic design and manufacturing tools. All these technological endeavors have

brought down associated costs and are quickly becoming commercially available. Unmanned aerial vehicles are used in agricultural applications, have flown into restricted air space, have been used to smuggle illegal and prescriptive drugs across borders. Like the cell phone and the personal computer of the past, the potential exists in scaling the size down to the point of manipulating particles that are measured in nanometers, in other words, one billionth of a meter and greater autonomy. Nanotechnology exists, but many technology analysts believe nano-robotics is in the not too distant future. Prototype robots scaled down to the size of insects or a small fish already exist for the purpose of observing. A future enabler to robotic capability is Three-dimensional printing. Three-dimensional printing is a form of robotics. Like an inkjet printer uses coats of ink to create an image or words on a page, a 3D printer uses preloaded materials like plastic or polyurethane or metal to make a shape in a layer-by-layer process.

In the near future, a perpetrator could download the design for a robot and print the key components, assemble them and build a fully functional autonomous insect-size drone capable of identifying its target—armed with a radioactive, chemical or biological element tipped stinger—and delivering a non-attributable injection.

Within the field of life sciences, innovation is rapidly occurring in two areas. One area is the gene sequencing capability that makes it cheap, faster, and easier to decipher the genetic code or DNA of all life forms to include most viruses. In 2002, researchers announced they had synthesized the complete poliovirus in three years. Oneyear later a different group of researchers were able to synthesize a similar viral genome in only two weeks.[8] In 2015, during an American Society for Microbiology research meeting in Washington D.C, a panel consisting of Homeland Defense and the FBI science experts had concluded their discussion by unanimously concurring that the next Bill Gates or Steven Jobs and the next big transformative change in technology would occur in the fast growing realm of life sciences.[9] Fast growing, as in exponentially fast; one Bioterrorism expert likened the proliferation of gene-synthesis capability as the same as the growth in computer technology power, which continues, to double every two years.[10] The transformation could possibly come from a "garage biotech amateur," a top global pharmaceutical company, or a university. The second area where Biology is rapidly growing is in "Gain of Function" (GOF). GOF is the process of artificially creating a virus strain far more virulent to a living organism within a controlled environment to better understand interaction in humans.[11] Scientists use GOF in order to create vaccines that stop the spread of mutating viruses.

By 2030, analysts believe the advancement of scientific discoveries and technologies, combined with the convergence of chemistry and biology will produce weapons with more useful characteristics than currently available. Given the global security environment, consequences of these forms of technology in the hands of somebody with malicious intent is astonishing, and deserves consideration in planning at the strategic and operational levels.

For example, with today's technology, the means to acquire and weaponize naturally occurring pathogens are increasingly available and in more readily useable forms for state and non-state actor's alike.[12] Geo-tagging images commonly occur over the Internet. Individuals interested in harvesting pathogens from nature to the specific source of virulent disease outbreaks can use images posted as part of reporting over the internet.[13] In 1995, the American Type Culture Collection (ATCC), a nonprofit repository for bacteria cultures, shipped a culture of Yersinia pestis, more commonly known as the "bubonic plague" to an activist using a falsified institution certification number.[14] In 1998, the FBI arrested the same individual again for a strain of Anthrax.[15]

Just over fourteen years ago, one week after the 9/11 attacks by terrorists, America experienced an Anthrax attack on members of Congress and Media outlets. The perpetrator(s) used the postal system for delivering the Anthrax spores and sealed letters. Consider the implications of security if the perpetrator(s) utilizing today's available off the shelf or do-it-yourself homemade drone with GPS and an agricultural applicator technology.

Another disconcerting matter about biotechnology is tracing it back to an attacker or perpetrators. In the example of the 2001 anthrax attack, it took seven years after the event to build a case against a possible lone

perpetrator.[16] As U.S. enemies continue to be largely non-state actors, this difficulty of tracing is going to consume a larger portion of our efforts.

Another concern is the potential for overreaction by the public which could result in policymakers placing moratoriums on science. In 1999, the West Nile Virus (WNV) outbreak had occurred in upper New York. WNV was never seen before in the Western Hemisphere. A few months prior to the WNV outbreak an Iraqi defector claimed that Saddam Hussein was weaponizing the West Nile Virus. This rumor was sufficient enough for public health authorities to respond as if it were a bioterrorism attack.[17] Officials did eliminate the possibility of a bioterrorist attack. Eventually, genetic sequencing did determine the WNV in New York was a mutated strain found in Israel. Even today, within some scientific communities it is thought that the attack was meant to mimic a natural outbreak.[18] Mr. Bill Gates' worst nightmare scenario is a pandemic outbreak similar to the Spanish influenza of 1918.[19] Consider for a brief moment if, through GOF, a pandemic event was intentional with only certain populations vaccinated.

Cast of "most likely" Culprits and their Characteristics

Technology in itself is beneficial to the global community. New technology has certainly outweighed the security implications in most cases. However, within the global community there are many forms of agitators, state sponsered militia organizations, non-state terrorists, cyber criminals, gangs, and other transnational criminal organizations that have become and are becoming empowered with cheap new technology and information.

In March, the co-founder and chairman of the social media site Twitter had his life threatened by the self-proclaimed Islamic State of Iraq and Syria (ISIS) supporters for shutting down their accounts.[20] ISIS understands the importance of social media and the Internet to get their strategic narrative out to the world. As the world recently witnessed, threats need to be taken seriously. For example, the Al Qaeda sympathizer terrorists attacked the offices of the satirist magazine *Charlie Hebdo* in France last January.

The State Department and intelligence agencies consider ISIS more united in their vicious attacks using terrorist techniques. ISIS has demonstrated the ability to inspire lone wolf attacks and recruit through social media. Intelligence analysts estimate that about 20,000 foreign fighters from approximately a hundred different countries are currently supporting ISIS in Iraq and Syria. Some foreign fighters will return to their home countries.

In his book *A Brave New War*, John Robb refers to this new threat as an "autonomous loose, self tuning network of global guerillas" because they represent a broad-based threat that far exceeds that offered by terrorists or guerillas in the past.[22] According to John Robb, it is likely that the United States military forces will find it fighting a thousand tiny armies.[23] Military historian and author Dr. Max Boot wrote a book that outlined a comprehensive historical point of view on guerilla and insurgencies, *Invisible Armies*,[24] discussing the tactics typical of guerilla warfare and insurgencies.

The University of Stanford's Center for International Security and Cooperation maintains an active database of over 100 militant organizations throughout the world.[25] Based on future population predictions the amalgamations of these types of organization coupled with the rapid advancement of technology will challenge and likely erode existing national and international security platforms. These "invisible armies" will reside among the people, hidden in one of three-dozen mega cities by 2025.[26]

To illustrate the potential effect of a non-traditional or non-state actor on a society, one only has to look at the island nation of Jamaica that has an estimated eighty-five gangs with a membership range of 2,500 to 20,000 people.[27] The reputation of the Jamaican "posses" is one of absolute ruthlessness and high efficiency in pursuit of their territorial and commercial interests.[28] With a population of approximately 2.7 million people, the number of murders and other violence puts Jamaica in the top five tiers of the highest per capita homicide rates in the world.[29] The Jamaican military, consisting of 3,000 personnel and Jamaican law enforcement agencies, are ill

dvised to enter neighborhoods controlled by Jamaican gangs.

The University of Stanford's Center for International Security and Cooperation maintains an active database of over 100 militant organizations throughout the world.[25] Based on future population predictions the amalgamations of these types of organization coupled with the rapid advancement of technology will challenge and likely erode existing national and international security platforms. These "invisible armies" will reside among the people, hidden in one of three-dozen mega cities by 2025.[26]

To illustrate the potential effect of a non-traditional or non-state actor on a society, one only has to look at the island nation of Jamaica that has an estimated eighty-five gangs with a membership range of 2,500 to 20,000 people.[27] The reputation of the Jamaican "posses" is one of absolute ruthlessness and high efficiency in pursuit of their territorial and commercial interests.[28] With a population of approximately 2.7 million people, the number of murders and other violence puts Jamaica in the top five tiers of the highest per capita homicide rates in the world.[29] The Jamaican military, consisting of 3,000 personnel and Jamaican law enforcement agencies, are ill advised to enter neighborhoods controlled by Jamaican gangs.

This shift in authority has impaired the traditional distinction between law enforcement and military national security functions, essentially eliminating the sovereignty of the state and the personal security of the Jamaican citizens. The Jamaican gangs have been so effective, other democratically elected governments in the Caribbean contend that the gangs are profiting from globalized operations, making Jamaican gangs a transnational criminal organization. Jamaican gangs are enhancing their capabilities through knowledge gained from the Internet.

According to an FBI 2011 National Gang Threat Assessment, gangs in general, are expanding, evolving and posing an increasing threat to U.S. communities.[30] Gangs are becoming more adaptable, organized, sophisticated, and opportunistic, exploiting new and advanced technology as a means to discretely communicate, target rivals, and extend their criminal activity as well as recruit. Gangs are engaging in crime such as counterfeiting, identity theft, and mortgage fraud, primarily due to the high profitability and much lower visibility and risk of detection and punishment than drug and weapons trafficking.[31] Gang members within some North American correctional facilities are adopting radical religious views while incarcerated. Gangs in the western hemisphere encourage members, associates, and relatives to obtain law enforcement, judiciary, or legal employment in order to gather information on rival gangs and law enforcement operations, gang members have infiltrated the U.S. military.[32]

In the future, gang members will likely seek to acquire weapons they can sell on the black market. Also noted in the National Gang Threat Assessment, is that most North American gangs have ties to "Criminal Organizations" throughout Mexico, Central and South America. A correlating effect of the smuggling network has been overwhelming and corrupting government officials around the world to various degrees. It is estimated the global smuggling network has a value of one to three trillion U.S. dollars and is supplying the huge demand in the developed world with drugs both recreational and pharmaceutical knockoffs, weapons of all variations to include man portable air defense systems (MANPADS), technology, intellectual property, undocumented workers and money laundering.[33]

In some cases, as mentioned with the Jamaican gang and other gangs throughout the world, transnational crime have aided gangs to take control of a state or establish a "shadow" government or quasi state region. Another lesser-known example of a quasi-government is in a place called "Transdniester". Transdniester is breakaway region on the Eastern border situated between the Moldovan Republic and Ukraine. Transdniester has established its own government, army, and other foundations of being a state although not being recognized by a single country. According to an editor at Foreign Policy, Moises Naim, states "weapons to Transdniester is what chocolate is to Switzerland or oil is to Saudi Arabia."[34] Transdniester has vast stockpiles of Soviet shells and rockets. Transdniester manufactures new machine guns, rocket launchers, rocket propelled grenades (RPG's) and other weapon systems.

Neither of the legitimately recognized governments of Jamaica or Moldova has the political will or capacity to manage criminal elements. These criminal organizations are continuously seeking partners to expand through cracks in the security system.

When one examines the battlefields of Iraq and Syria there is a union of criminals, fundamentalists, and tribal groups instead of a single army with a single goal. All are in competition with each other but are willing to work together to fight the United States and its Western allies by developing a market that advances the wealth of all by attacking infrastructure, using technology to network with other like-minded individuals, and as we have seen more frequently attacks similar to those in New York in 2001, Madrid, Spain in 2004, France in January, 2015, and the failed attack on a conference in Dallas, Texas which was inspired by the attack on *Charlie Hebdo*. Between 1970 and 2013, there were over 125,000 terrorist attacks.[36] The National Consortium for the Study of Terrorism and Responses to Terrorism at the University of Maryland has assessed a worrisome trend. Terrorist attacks have continue to rise and increased by 35% in 2014 from the previous year.[37] Terrorists, comparable organizations, and loan wolf's do not factor in opposition by State military forces or the billions (and in the case of the U.S., trillions) of dollars spent on defense over the last two decades because terrorists, unlike traditional armies, look for softer targets such as non-combatants and unprotected infrastructures, as is evident by recent attacks.

Through the Internet, cell-phones, and social media applications the world witnessed a number of events that led to violence and capitulation of governments in North Africa, Middle East. In more recent months terrorist organizations and lone wolf actors have attempted to employ this tactic all around the world in order to bring attention to their cause and destabilize or project the inability of a Government to protect its citizens. Although these terrorist actions appear to have little success in and of themselves, it demonstrates the vulnerability that is being faced by nations, of all types, with a problem that continuously festers over time. New technologies such as UAVs and biotechnology in the wrong hands will be costly to defend against. Over the next few years, the U.S. military is likely to come in contact with non-state actors with malign intent who attempt to capitalize on the narrative against the United States or its allies and their ability to prevent, protect, and provide for the safety of its citizens or secure the supply of public goods most citizens are accustomed to.

The Chairman Joint Chief of Staff, General Dempsey stated in the *National Military Strategy 2015*, "Today's global security is the most unpredictable [I have] seen in 40 years of service."[38] Global insecurity and volatility will increase in the future because of rapid advancement and distribution of technology that has the potential for dual purpose through a growing global interconnectedness accessed by shifting populations with violent extremists, trans-regional criminals and other perpetrators who seek to destabilize existing government. As the *National Military Strategy 2015* emphasizes, the United States and its allies will need to attract men and women who are willing to join the military that are comfortable and familiar with the technologies of today and of the future. They will need to reshape the force structure in order to combat the future threats.

Lieutenant Colonel John Nolan, U.S. Army Reserve, is currently the Branch Chief for HQDA G4 Logistics Operations Center. He holds a B.A. from the University of Central Florida and an M.S. from the Florida Institute of Technology. Lt. Col. Nolan has served with the 143D ESC, Logistics Civilian Augmentation Program (LOGCAP), SDDC, Special Operations Command, 311 ESC, and the Office of the Chief Army Reserve. He also taught ROTC at Jacksonville State University, Alabama.

NOTES:

1. Joint Chiefs of Staff, *National Military Strategy of the United States 2015* (June 2015), 6-7, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

2. Benjamin Wittes and Gabrelli Blum, *The Future of Violence, Robots and Germs, Hackers and Drones* (New York: Basic Books, 2015), 22.

3. David Rothkopf, "From the Shores of Tripoli," *Foreign Policy* (May/June 2015): 77.

4. BBC, "Military Fears over Playstation2" BBC News online, April 17, April 2000, http://news.bbc.co.uk/2/hi/asia-pacific/716237.stm.

5. Daniela Rus, "The Robots Are Coming; How Technological Breakthroughs Will Transform Everyday Life," *Foreign Affairs* (July/August 2015): 3.

6. Michael C. Horowitz, "The Looming Robotics Gap," *Foreign Policy* (May/June 2014): 64.

7. Ibid., 66.

8. Wittes and Blum, *The Future of Violence*, 26.

9. Vincent Racinello, Maria Julia Marinissen, Edward H. You, and David R. Howell, "Careers in Biodefense," Microbe World online, This Week in Microbiology podcast 99, March 4, 2015, 59 min, http://www.microbeworld.org/podcasts/this-week-in-microbiology/archives/1859-twim-99-careers-in-biodefense.

10. Wittes and Blum, *The Future of Violence*, 27.

11. Laurie Garrett, "Biology's Brave New World; The Promise and Perils of the Synbio Revolution," *Foreign Affairs* (Nov/Dec 2013): 32.

12. John P. Caves Jr. and W. Seth Carus, *The Future of Weapons of Mass Destruction: Their Nature and Role in 2030*, Occasional Paper 10 (National Defense University Press, June 2014), 27.

13. Ibid., 27.

14. David P. Clark, *Germs, Genes & Civilizations* (Pearson Education, 2010), 132.

15. Ibid., 133.

16. Dan Vergano,"Strides in Biodefense Follow 2001 Anthrax Scare," and "Anthrax Timeline," *U.S. Today*, September 30, 2011.

17. Madeline Drexler, *Emerging Epidemics; The Menace of New Infections* (Penguin Books, 2010), 53.

18. Ibid., 54.

19. Ezra Klein, "The Most Predictable Disaster in the History of the Human Race," *Vox*, May 27, 2015, http://www.vox.com/2015/5/27/8660249/gates-flu-pandemic

20. John Robb, "It's Open Season on the Tech Elite," Global Guerrillas blog, March 2, 2015, http://globalguerrillas.typepad.com/globalguerrillas/2015/03/its-open-season-on-the-tech-elite.html.

21. Chairman of the House Armed Services Committee Mac Thornberry, "Weekly Republican Address: Honoring our Commitment to our Troops," May 22, 2015, http://www.speaker.gov/press-release/weekly-republican-address-honoring-our-commitment-our-troops.

22. John Robb, *A Brave New War* (John Wiley & Sons, 2007), 40.

23. Ibid., 212.

24. Max Boot, *Invisible Armies; An Epic History of Guerilla Warfare from Ancient Times to Present* (Liveright Publishing Corporation, 2013), 3.

25. Martha Crenshaw, "Mapping Militant Organizations," Center for International Security Cooperation, accessed 27 July 2016, http://cisac.fsi.stanford.edu/research/mapping_militant_organizations.

26. Mega-City is defined as an urban center with more than 10 million inhabitants. See Jonathan Kalan, "Think Again: Megacities," *Foreign Policy* (May/June 2014): 69.

27. Max G. Manwaring, *Gangs Pseudo-Militaries and Other Modern Mercenaries; New Dynamics in Uncomfortable Wars* (University of Oklahoma Press: Norman, 2010), 26.

28. Ibid., 26.

29. Vincent Cooper, "2013 Jamaica Crime and Safety Report," Bureau of Diplomatic Security, United States State Department of State, OSAC.

30. National Gang Intelligence Center, "2011 National Gang Threat Assessment - Emerging Trends", FBI, 3, accessed 27 July 2016, https://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment.

31. Ibid., 9.

32. Ibid., 10.

33. Robb, *A Brave New War,* 220.

34. Moises Naim, *Illicit; How Smugglers, Traffickers, and Copycats are Highjacking the Global Economy* (Doubleday, 2005), 57.

35. Ibid., 58.

36. "Global Terrorism Database," National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland, last updated June 2016, http://www.start.umd.edu/gtd/.

37. House Armed Services Committee, William Braniff, *What is the State of Islamic Extremism: Key Trends, Challenges and Implications for U.S. Policy*, 114th Cong., 1st sess., 13 February 2015, 3-4.

38. Gen. Martin Dempsey, Chairman, Joint Chief of Staff, *National Military Strategy 2015* (June 2015), Chairman's Foreword, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.