Volume #3: Escalating Conflicts Globally

Summary of Key Findings:

- Budget tightening is shifting the focus of U.S. national defense spending towards technology.
- The U.S. led global defense procurement in 2014 with 37.8%, followed by China, 9.7% and Russia, 4.5%[1].
- Malicious cyber traffic is visible on 100% of networks, increasing the need for cybersecurity solutions[2].
- The North American cybersecurity market is expected to grow at a 17.4% rate (2010-2020)[3].
- Seven U.S. cities will likely be considered well-developed "Safe Cities" by 2025, combining technology and best practices to enhance public safety[4].
- City Cloud Solutions for data collection and analysis are expected to have the greatest impact on growth of "Safe Cities"[4].

As a continuation of our discussion related to factors of influence that we see shaping the investment landscape over the next several years, we would like to delve into our next important factor, escalating global conflict. Unfortunately, conflict both at home and abroad is the new norm. It seems as if every day there is an unfortunate episode of violence due to a litany of conflicts including: the Civil War in Syria that has created a major refugee crisis in Europe and soon could become a reality here in the U.S.; the War against ISIS which has been the linchpin to a number of terrorist attacks in the Western world either through direct sponsorship or radicalized domestic terrorists; tensions in the South and East China Sea, the North Korean crisis, the reemergence of the Taliban in Afghanistan, the conflict in the Ukraine, criminal violence in Mexico, the ongoing Israeli-Palestinian conflict, the conflict between India and Pakistan, and the War in Yemen and Boko Haram in Nigeria to just name a few. As the world's de facto guardian of peace, any and all of these conflicts could affect U.S. interests and thus are likely to necessitate a response. Current U.S. military strength could be greatly diminished by having exposure to multiple regional conflicts at once. In addition, the effects of the budget sequester on the US military capabilities has been substantial. Both President-elect Donald Trump and the Republican-controlled Congress have indicated the urgent need to reverse this trend.
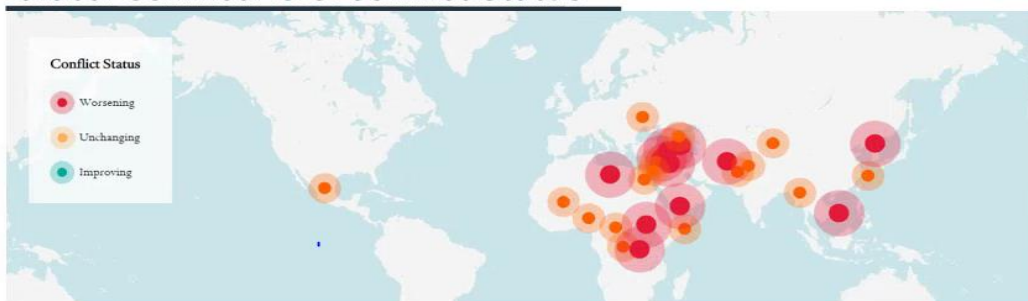

Image from Council on Foreign Relations website: http://www.cfr.org/global/global-conflict-tracker

National Defense Will Focus on Non-Traditional Actors[5]

National defense will continue to shift away from defense against nation-to-nation warfare, instead focusing on countering attacks from non-traditional actors, such as terrorist organizations and cyber hackers.

National defense efforts will continue to pursue solutions to prevent violent extremism – both within the U.S. and abroad – through military and foreign policy means. In addition, the emerging threat of cyber terrorism will be an increasing concern for national defense. As connectivity expands, especially into more and more physical objects and critical infrastructures, there will be greater demand for improved counter measures to prevent and mitigate the effects of cyber terrorist attacks aiming to control or destroy physical assets.

U.S. Department of Defense Budget 2014-2020
($ in billions)[6]
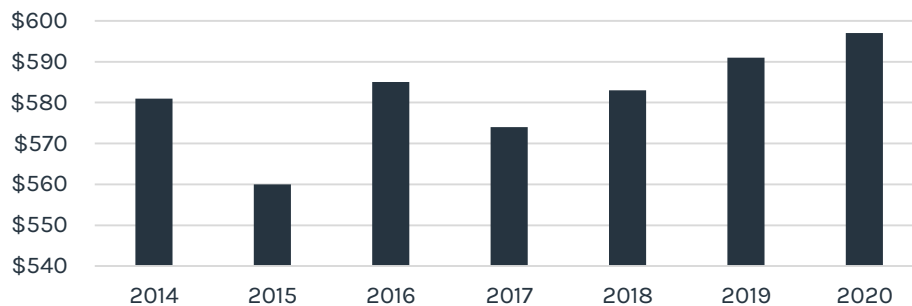
As countries develop greater offensive cyber capabilities, state-sponsored cyberattacks and espionage against the U.S. will likely increase through 2025. Countries such as North Korea, Iran, Russia, and China will seeks to further economic and foreign policy objectives by targeting U.S. government, military and private sector networks. However, distinguishing between state-sponsored cyber activity and the actions of criminal or terrorist organizations within that nation's borders will continue to prove difficult, challenging the U.S. and international organizations to clearly define acts of cyber warfare, as compared to cyber-crime.

Globally, political instability may increase in regions with weakened governments, sectarian divisions, and/or wide economic disparities among social groups. The U.S. will likely continue to contribute military assistance when multi-lateral intervention efforts further U.S. interests abroad and are supported by the majority of the international community. Despite high tensions with countries such as North Korea, Iran, Russia and China, a direct military confrontation between the U.S. and another nation is unlikely.

A slimmer U.S. defense budget will focus spending on technology to support operations against non-traditional actors, expanding opportunities for companies in the defense contract space. Between 2014 and 2020, U.S. defense spending is expected to grow at 0.5% CAGR, increasing at a much lower rate than in previous years[6]. Despite budget tightening, the U.S. is expected to remain the global leader in defense spending through 2020.

Changing Focus of U.S. Defense Spending[7]
The new era of defense spending will focus on four main objectives: 1) Modularity, 2) Sensors, 3) Data Handling and Analysis and 4) Unmanned everything. Design and capabilities that accomodate multiple systems (i.e. common surveillance and reconnaissance packages for use in multiple platforms) will see increased demand for their systems. Sensors with improved reliability, enhanced performance, and that allow for predictive maintenance as well as forward area, battle area, and

operational intelligence will receive a larger portion of the defense spending budget. Analysis of huge amounts of data will be essential. Currently, intelligence, surveillance, and reconnasisance operations in Afganistan alone generate more than 53 terabytes of data daily. The effective use of all that data can change the rules of engagement and make for more tactical and efficient military operations. Lastly, there is a movement towards increased integration of commerical off-the-shelf components with unmanned vehicle platforms with on-ground and maritime capabilities. Considering the repercussions of soldiers returning from the Middle East and the cost associated with their care, the reduction of the use of humans in direct conflict is not only saving lives but is also likely to save money.

Share of Total Defense Procurement Spending - 2014

U.S. 37.8% China 9.7% Russia 4.5% Rest of the World 48.0%
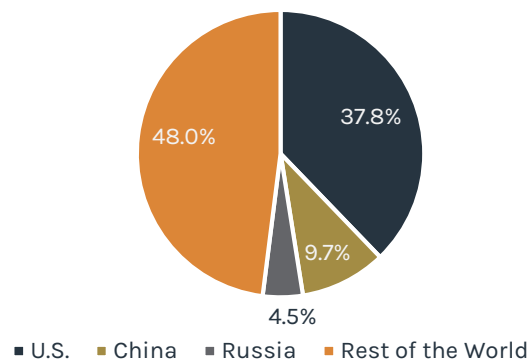
Real world examples of the growing influence of technology companies in U.S. defense contracting can be found by recent acquisitions, such as Raython's acquistion of Websense to increase their cyber capabilities, Google's acquistion of Titan Aerospace to expand aerial drone offerings and Boeing's acquisition of 2d3 Sensing to improve their imaging and video analysis capabilities. 3RC will pay special attention to opportunities were consolidation by large technology or defense contractors is occuring.

What does this all mean to 3RC Investors?
In the next several months, 3RC will continue its study of this factor of influence by focusing on all of the implications that may arise, including opportunities in cybersecurity, video and surveillance equipment, robotics and particular opportunities in the U.S. defense spending budget where consolidation is occurring. This factor of influence is one that is most fluid in that it can change in a flash based on the actions of foreign actors, so we must be flexible in our analysis to focus on areas of the markets that will be impacted long term and not be tempted by attractive novelties.

SOURCES:
1- *Frost & Sullivan*
2- *Pew Research Center*
3- *Financial Times "Cisco Warns of 'unprecedented growth' in cyberattacks"*
4- *Police Executive Research Forum*
5- *Worldwide Threat Assessment of the U.S. Intelligence Community, 2015*
6- *U.S. Department of Defense*
7- *Center for Strategic and International Studies*