Volume 1, Issue 6

OCTAVIAN REPORT

The Octavian Report: January 2016

EMERGENT WEAPONRY AND THE NEW (AB)NORMAL

BY DEE SMITH

The battlefields contemporary military contests take place on are changing. Governments will continue to struggle for supremacy on land, sea, and air, but non-traditional actors — be they ISIS or high-level hackers — have better access to and understanding of how technology can have a huge and deadly impact on our highly networked world. Even as the Chinese debut a new class of missile, threats from far less entrenched centers of power continue to grow.

On September 5, during celebrations commemorating victory over Japan in World War II, the Chinese government premiered its new "carrier killer," the DF-21D anti-ship ballistic missile (ASBM). Although the existence of the missile was known in military and intelligence circles — its production and deployment having been reported as early as 2010 — this was nevertheless a provocative display. It was intended as a direct challenge to U.S. military dominance in the Pacific. Could there be, after all, any reason to produce a carrier killer other than to challenge the one nation that has a large number of operational aircraft carriers?

As ostentatiously powerful as such a weapon is, it represents nonetheless the rear guard in the field of emerging weapons technology — a field where the end user of a weapon matters almost as much as the nature of the weapons itself. And one of the most disruptive elements of the emerging weapons dynamic is the disequilibum that it produces due to the fact that many such weapons can be deployed by non-state actors. These are groups, organizations, or individuals that have the ability to act with consequence geopolitically and do not ally themselves with any "formal" or traditional state or country — and serious observers need to be aware of the interplay between new tech, new battlefields, and new actors.

Cyber weapons highlight this need perfectly. In our networked world, where more and more of our economic, social, and political existence — and indeed our critical infrastructure — depends on computer systems, it is clear that cyber weapons pose a mounting threat. Unlike carrier killer missiles and other systems that can in practice only be developed by large states with commensurate military R&D budgets and facilities, cyber weapons can be developed and deployed by anyone with the requisite skills and an Internet connection (or anyone with knowledge and money to hire such an individual or team). And the attacks launched by these rogue actors can be devastating.

Many such incidents remain classified or highly confidential, but the attack mounted on the Iranian nuclear program by a computer worm called Stuxnet (said but never officially confirmed to have been developed by the U.S. and/or Israel) is public knowledge. This worm attacked specific computers in Iran throughout 2010 and 2011. What is notable about it is that it was the first open example of software that caused significant physical damage to systems in the "real world." In the Stuxnet case, the worm very precisely singled out and attacked supervisory control and data acquisition (SCADA) systems of Siemens Step 7 software, systems that monitor and control centrifuges, including those used to produce nuclear material. In addition to collecting and realying information, the infection made Iranian centrifuges tear themselves apart. However, the worm infected many additional computers in countries including Indonesia, India, and even the U.S., serving as an exemplar of the uncontrollable nature of even the most precisely targeted cyber attacks. These threats are growing dramatically, and are so dire that a senior defense expert recently stated off the record that "the truth is that no organization today can fully protect itself" from them.

In other words, the "hacking gap" — a term to denote the difference in capability between the military and political establishments and the young and disaffected, typically male, and sometimes radicalized individuals behind cyber attacks — needs to be addressed post-haste. Not least because it is often not clear who the adversaries really are in this new operational landscape. Analysts put the percentage of unknown attackers as high as 27 percent. And while the targets of the attacks — largely governments and big businesses — typically act in a defensive and reactive mode, their attackers are proactive and innovative.

> "The end user of a weapon now matters almost as much as the nature of the weapons itself."
>
> —*Dee Smith*

This gives them an advantage, one compounded by the lack of transparency typically practiced by governments and businesses about attacks (in many cases not revealing that such attacks have happened). In contrast, non-state actors chatter with each other constantly. Such non-state actors comprise strange bedfellows, ranging from religiously or politically motivated extremists to criminals who think only of financial gain, a great many of whom vigorously share information despite their differing ideologies. That lack of boundaries cuts both ways, however. Some non-state actors are targeting other non-state actors: Anonymous has recently said it is undertaking rolling cyber attacks against the Islamic State.

Government intelligence agencies have a disposition against sharing information because it is perceived to compromise sources, methods, and tradecraft, and as a result to devalue the intelligence — a genuine concern. However, this limits their ability to respond. As a result, incumbent actors such as governments are constantly behind the curve in fighting off cyber attacks. The situation is even worse in the commercial world, where the term "digital vortex" is sometimes applied to the lack of understanding that large corporations often have about what is happening around them in the cyberspace that they themselves inhabit and depend upon.

To use military terms, these phenomena constitute asymmetric and asynchronous warfare: asymmetric because very small actors can have very large effects, and asynchronous because the attack and counterattack can be widely separated in time. Although incumbents have resources many orders of magnitude in excess of non-state actors, in the hyperconnected world we have created, those on the fringes have greater power to disrupt .The empowerment of the small actor is a key feature of our time, and the emergence of many classes of new weapons is further increasing their reach.

Take drones. When we think of drones used in warfare, we typically think of those engineered specifically for the task and deployed by large states. These represent in themselves an emerging class of weapons, and one that allows an actor such as the U.S. to engage with an enemy without putting any lives at risk. Drones that surveil or track and fire on targets in Afghanistan can be controlled by a pilot sitting in front of a computer screen in Florida, literally half a world away.

But imagine an airspace in the near future saturated with drones (ranging from police and internal security drones to those being contemplated by Amazon and WalMart for delivery of purchases, as well as "amateur" civilian drones) — any of which could be hacked. The scope of the problem facing us if this becomes reality is soon apparent. The fact that an actor from another state or a terrorist sitting halfway across the world could hack such drones and use them for crude but effective attacks (which could include simply causing numbers of drones to crash unpredictably, perhaps in tandem) is a demonstration of the fact that the more we deploy complex and interconnected technology, the more we make ourselves increasingly vulnerable. But even de-networking would be of limited help here: malevolent actors do not even need to hack military drones to use drones as weapons. Commercially available civilian drones can be converted into capable tools for surveillance and even for attack — and now have ranges up to three miles from the originator.

The hijacking of technologies for alternative violent use is not limited to drones. One under-discussed issue in the fight against ISIS is that the group has probably harvested enough radioactive medical materials from hospitals in areas that they have occupied to make several dirty bombs. While the physical and even health-related effects of a dirty bomb might in the event of its deployment be quite minimal, the financial damage could be devastating if one were detonated in a densely populated major financial center, effectively reducing to zero the value of many square blocks of valuable real estate. This is yet another example of the fragility of a hyperconnected system.

The emergent weapons described here are only the tip of the iceberg. From autonomous military robots to bio-weapons, an increasingly diverse panoply now sits at the fingertips of a pullulating group of actors incumbent or fringe, known or unknown. We have entered the era of irregular warfare and exotic weaponry, and it will be an era dominated by the most innovative designers, resource-managers, strategists and tacticians — no matter whom they happen to be fighting for.

Dee Smith is the founder and CEO of Strategic Insight Group.