AMERICAN FOREIGN POLICY COUNCIL


# Defense Technology Monitor: No. 1

February 18, 2016 **Richard M. Harrison**, **Paige Rotunda**

**Related Categories:** Cybersecurity and Cyberwarfare; Energy Security; International Economics and Trade; Military Innovation; Science and Technology; China; Russia; Ukraine

**LEGAL QUESTIONS ABOUT LASER WEAPONS**
The growth and increasing popularity of laser weapons is generating new questions about their status under international law. A case in point is China's PY132 handheld laser gun - a weapon that was publicly displayed at the December 2015 police exposition in Beijing. The weapon's projected uses include the blinding of enemy tank thermal/night imaging sensors and countering drones. However, they rub up against the provisions of the 1998 Protocol on Blinding Laser Weapons, which prohibit the use of weapons like the PY132 against manned vehicles such as helicopters and planes, whose pilots can be blinded by lasers. For its part, the Chinese government has not disclosed the planned uses of the PY132 and other laser weapons now under development. (*Popular Science*, January 7, 2016)

**RUSSIA'S A2AD STRATEGY**
Russia has long been a vocal opponent of U.S. and European missile defense plans. Yet the Kremlin is quietly expanding its own anti-missile capabilities. Russia's military is slowly and deliberately deploying a missile defense architecture of their own making in several global hotspots, including its recently-annexed Crimean Peninsula, the Russian enclave of Kaliningrad (situated between Poland and Lithuania), and in Syria. Gen. Frank Gorenc, the Commander of United States Air Force operations, has warned of Russia's growing ability to restrict NATO member state access airspace in Europe as part of what he and other military officials term a new anti-access/area denial (A2AD) strategy. "They've increased capacity, they've increased capability, and, by the way, have demonstrated a willingness to use it," Gorenc has said. (*New York Times*, January 11, 2016)

**NEW DRONE CAPABILITIES NEEDED**
Faced with dwindling budgets, the U.S. Army is attempting to strike the right balance between fiscal austerity and the capabilities of both manned and unmanned aerial systems (UAS) for new missions. Army aviation chief Maj. Gen. Michael Lundy has acknowledged that, while there are ways for the military to make more efficient use of the "thousands" of drones already in its arsenal, new missions are increasing the need for more capable systems. "I don't want to be on runways anymore," Lundy told a recent Association of the United States Army conference. "[A future drone] needs to have a VTOL [vertical take off and lift] capability. We've got to be able to push it forward with units. It can't be sitting at an airfield four hours away... It's got to be survivable, so we've go to reduce the signature. And we've got to reduce how many people it takes to run it." (*Breaking Defense*, January 14, 2016)

**HARDENING FUTURE FIGHTERS**
Despite the relative newness of the F-22 "Raptor" - which was delivered to the U.S. Air Force in 2012 - debate is already heating up on Capitol Hill about the next generation of fighter jets, and the types of technology and mission requirements for these sixth-generation aircraft. Several areas of improvement have already been flagged, among them thermal management at high speeds (potentially supersonic) for directed energy weapon systems. Another key issue now receiving attention from both lawmakers and industry is the question of cyber resiliency - and how emerging fighter aircraft can best be protected against cyber intrusions or attacks that can compromise their missions and functioning. (*Defense News*, January 15, 2016)

**HACKERS TURNED OUT THE LIGHTS IN UKRAINE**
At the end of December, some 80,000 Ukrainians found themselves without power for several hours due to a cyber attack on two power distribution companies. Ukrainian officials have blamed Russia for orchestrating the attack, and for good reason. Based on the timing of the incident, it appears to have been retaliation for the physical shutdown of power stations providing electricity to Russia's Crimean Peninsula by pro-Ukrainian activists.

Remotely causing physical damage to a power plant is nothing new. In this instance, however, hackers did not do physical damage but instead temporarily shut down power at the facilities. They also launched a denial of service attack on the utility call centers of the relevant power company, so that customers could not alert operators to service interruptions. The attackers likewise deployed malware onto the power company computers that erased the ability of the users to get the systems back up and running. (*Wired*, January 20, 2016)

© 2022 - American Foreign Policy Council