



Defense Technology Monitor: No. 21

September 25, 2017 **Richard M. Harrison, Andrew Greenman**

Related Categories: Cybersecurity and Cyberwarfare; Military Innovation; Missile Defense; Science and Technology; China

U.S. NAVY 3D PRINTS SUBMERSIBLE

Three-dimensional printing continues to revolutionize manufacturing for both civilian and military affairs by offering timely, cost effective solutions to expensive acquisition challenges. The U.S. Army has already managed to successfully print a grenade launcher, potentially revolutionizing supply chain logistics for deployed infantry units. (See *Defense Technology Monitor* No. 16) Now, researchers from the Naval Surface Warfare Center (NSWC) and Carderock Division's Disruptive Technology Laboratory (DTL) have gone one step further and developed a 3D printable submersible.

The Navy team used a room-sized printer at the Department of Energy's Oak Ridge National Laboratory to print a 30-foot carbon fiber hull of a submersible similar to one currently used by Navy SEAL operators. While the initial proof of concept model isn't yet ready for operational testing, the Department of Energy says the production process cost only 10 percent of conventional manufacturing techniques and took days instead of months to complete. The team's next project is to produce a watertight version of the hull for further testing. Developers hope to have fully operational prototypes ready for real world use by 2019. (*The Verge*, July 29, 2017)

HAS CHINA DEVELOPED "HACK PROOF" COMMUNICATIONS?

China's burgeoning space and cyber capabilities have taken yet another step forward in recent weeks. Chinese state media has announced that, on the heels of the launch of the first quantum satellite last year, Chinese scientists have successfully used quantum key distribution technology to transmit "hack proof" communication several hundreds of miles from the satellite to multiple ground stations. If the reports are accurate, this is a significant accomplishment because it considerably complicates the ability of adversary nations to collect intelligence by intercepting communications between the satellite and ground stations. Reportedly, "once intercepted or measured, the quantum state of the key will change, and the information being intercepted will self-destruct." (Reuters, August 10, 2017)

A NEW WAY TO HACK COMPUTERS

As gene sequencing becomes increasingly common and gene editing techniques improve, creative scientists are testing ways to use DNA as a vehicle for data transmission. A group of Harvard scientists humorously demonstrated this in a June paper by storing a short animated video in DNA. Now, University of Washington researchers have turned the same techniques to a much more ominous purpose: inserting a virus into DNA and using it to attack computers sequencing that DNA. In this specific experiment, the researchers who inserted the malicious software were able to completely take over the computers in question. And while this experiment was deliberately rigged (with the target's security disabled and its sequencing software containing a vulnerability), the idea that malicious data could be stored on DNA and used to attack sequencing programs is troubling. The increasing speed and declining costs of DNA sequencing has made it widespread, and in the future hackers may be able to use blood or saliva samples to break into computer systems and networks in police forensics facilities, universities, or genetic labs. (*The Daily Dot*, August 10, 2017)

SELF-HEALING ROBOTS ON HORIZON

While still a long way from the liquid metal skin of science fiction robots like those in the Terminator movies, new developments in self-repairing synthetic skin may help robots recover from damage while working. Roboticists at the Vrije Universiteit Brussels (VUB), who specialize in the creation of "soft robots," recently released videos showcasing their newest project: a gel-like rubber polymer that melds together seamlessly when heated. The injuries inflicted on robots sheathed in the substance were realistic - one video shows the researcher slicing open a robot's finger with a scalpel. While the softness of the gel could make VUB's soft robots helpful in medicine and agriculture, the self-repairing ability of the skin and artificial muscle would be highly advantageous in combat scenarios as well. (London *Daily Mail*, August 17, 2017)

TECH LEADERS FIGHT FOR UN BAN ON KILLER ROBOTS

Famous inventor and entrepreneur Elon Musk, along with over a hundred robotics experts, has submitted a letter to the United Nations calling for an agreement banning lethal autonomous weapons. The group spearheaded by Musk argues that robots killing without human intervention is "morally wrong" and such weapons should be included (alongside landmines and fire bombs) under the 1983 Convention on Certain Chemical Weapons (CCW). In the letter, signatories stated that, "Once developed, [autonomous weapons] will permit armed conflict to be fought at a scale greater than ever, and at timescales faster than humans can comprehend."

In addition to worries over how autonomous weapons systems would be deployed, signatories also fear that such systems could be vulnerable to hacking, creating unintended consequences for their lethal capability. Several countries are developing lethal autonomous weapons, and an automatic border guard system deployed in South Korea can already kill automatically if its restrictions are removed. Governments fear falling behind in this burgeoning arms race, and fear that other countries will use the capabilities of killer robots against them - precisely the dynamic that the expert group is seeking to avoid. (*The Verge*, August 21, 2017)