Homeland Security
Science and Technology

Homeland Security Science and Technology Advisory Committee (HSSTAC) Quadrennial Homeland Security Review Subcommittee

Autonomous Technology White Paper

March 10, 2017

Homeland Security
Science and Technology

This publication is presented on behalf of the Homeland Security Science and Technology Advisory Committee, Quadrennial Homeland Security Review Subcommittee, Autonomous Technology, chaired by Mr. Daniel Dubno with contributions from Dr. Stephen Flynn, Dr. Yacov Haimes, Mr. Byron Collie as part of recommendations to the Department of Homeland Security, Under Secretary for Science and Technology, Robert Griffin (*Acting*).

<Signature on File>

_____

Daniel Dubno
Executive Director
Hourglass Initiative

HSSTAC Staff: Michel Kareis, HSSTAC Executive Director/DFO and Gretchen Cullenberg, QHSR Subcommittee support.

Homeland Security
Science and Technology

AUTONOMOUS TECHNOLOGY AND HOMELAND SECURITY

Mr. Daniel Dubno, Subcommittee Chair; Dr. Stephen Flynn; Dr. Yacov Haimes; and Mr. Byron Collie

Introduction

"Autonomous technology" is any kind of technology that can make complex decisions and function without being continuously directed and controlled by a person. Science fiction robots were once the sole examples of autonomous technology. Now autonomous control will redefine how objects and people move from place to place, how devices will care for people, and how they will provide services in factories, offices, residences, and healthcare facilities. Autonomous vehicles that can safely self-navigate between destinations will soon become a significant part of America's future infrastructure. Simple-to-program yet extremely powerful robots have become ubiquitous in factory assembly lines. Large warehouses now depend on robotic infrastructure to quickly move inventory. Nimble robots have moved to the home to perform menial tasks like cleaning floors and to provide care for bed-ridden patients. Arrays of autonomous flying, land-navigating, sea-navigating, and even submersible vehicles are also rapidly being developed and deployed. The term "drone" is being applied to many of these technologies. The risks associated with these technologies, however, have not been significantly addressed. While we have yet to see a major coordinated attack employing autonomous devices here in the United States, we cannot be complacent about this threat. As they become even more ubiquitous and integrated in our lives, their vulnerabilities will inevitably be tested and exploited with great potential for harm and social disruption. Autonomous machines can be hacked from remote locations. It may be difficult to track down perpetrators, especially if they are foreign entities**. Government and manufacturers must collaborate on stimulating and conducting R&D to deter avoidable tragedy by developing frameworks, architectures, and standards to mitigate the risk and must prepare for the consequences of misuse and attacks using autonomous technology.**

Some examples of autonomous technology are:

- **Self-driving cars and trucks**
- **Autonomous surface package delivery**
- **Unmanned Aerial Vehicles (UAVs)**
- **Industrial robots**
- **Home and hospital-care robots**
- **"Robotic" Sea-navigating Ships**
- **Autonomous Underwater Vehicles (AUVs), and Remotely Operated Vehicles (ROVs)**

There is a difference between "isolated autonomy" and "connected autonomy." Which of these systems pose greater risks for Americans and what intervention by DHS is required is difficult to predict at this time, but we contemplate some obvious threats and potential remedies below.

Autonomous vehicles will bring a host of benefits and concerns to society: significantly reducing accidents, eliminating unproductive human drive-times, empowering handicapped and elderly to travel more easily, while reducing effort and money spent on parking and even car ownership in large urban areas. At the same time, widespread adoption of autonomous vehicles is expected to displace hundreds of thousands of professional drivers who will have to find alternative employment. As transportation transforms, one of the biggest challenges society will face is autonomous vehicle cybersecurity and control.

At least in the near term, it appears that as autonomous vehicles add more capabilities to their electronic control units (ECUs), more hackable points of entry are introduced into increasingly complex computer control systems. (Most cars today have from 30 to 50 and as many as 80 ECUs with onboard computers accessing millions of lines of code.) As of now, no major malicious cyberattack on a vehicle has taken place that we know of. "But the potential danger was illustrated dramatically last year when two white-hat hackers remotely took control of a Jeep Cherokee and cut its transmission on the highway as part of a research initiative. The well-publicized incident prompted Chrysler to recall 1.4 million vehicles. Society is often reactive rather than proactive with security issues, adopting serious preventive measures only after a major incident has occurred." [1] (Hacked Volkswagen, Tesla, and Nissan Leaf cars have sparked concerns about the security of ever more connected and autonomous cars as well.)[2] **Separating entertainment control systems from critical life safety systems should be adopted by the auto industry in addition to adding layered security to the ECUs. DHS should join industry efforts to form an Automotive Information Sharing and Analysis Center (ISAC) which would focus on combatting vehicle vulnerability to hacking.** [3]

Autonomous cars and trucks can be programmed for good and ill. Such trucks and cars can deliver bombs without suicide-drivers or ram a high-value vehicle off the road and over a cliff. It would not require "hacking" of an autonomous vehicle to cause a profound terror attack. Vehicles that autonomously deliver tons of explosives or other weapons of mass destruction to a specific address at a designated time pose a very real threat. Trucks already capable of

[1] https://techcrunch.com/2016/08/25/the-biggest-threat-facing-connected-autonomous-vehicles-is-cybersecurity/
[2] http://www.autocar.co.uk/car-news/motor-shows-ces/harman-demonstrates-first-ever-live-car-hack-ces
[3] GAO REPORT: VEHICLE CYBERSECURITY: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack (GAO-16-350): Published: Mar 24, 2016. Publicly Released: Apr 25, 2016.

delivering tons of products (i.e., in late 2016, OTTO delivered 50,000 cans of Budweiser[4]) are being experimented with on our roadways and very soon it would take little expense, manpower, or sophistication to carry out massive attacks like the Oklahoma City bombing with trucks filled with explosives like Ammonium Nitrate (ANFO) or other agents. Authorized trucks carrying hazardous materials are particularly high value targets for terrorist hijacking or manipulation. **Techniques to protect crowds and high value targets from these threats must be considered including working with autonomous trucking companies and major carriers; devising methods for safeguarding and detecting lethal payloads through embedded and remote sensors; preventing the hacking and the manipulation of electronic manifests; restricting access by autonomous trucks to areas proximate to vulnerable high-value targets; and promoting technologies, such as automated barriers, geofencing, and sensors, for stopping such vehicles from being used nefariously.**

To crash into other cars, potentially kidnap people, and even disrupt our highway infrastructure does not require imagination or profound technological sophistication. Denial of service attacks (where autonomous cars can be reprogrammed to go where they are not welcome) is a topic about which much is still unknown, even among those working at the cutting edge of the industry. Hacking vehicle connectivity is a fairly new phenomenon and the technology continues to evolve rapidly. The ability to spoof the location, manifests, and weight of heavy-load carriers is of significant concern. It is also particularly important to secure vulnerable strategic choke points such as key bridges and tunnels from such autonomous vehicle attacks. With some degree of technological expertise, it is even feasible to convert a state-of-the-art autonomous electric car into a potential Electromagnetic Pulse (EMP) weapon given the energy potential of its battery system. Looking out towards a 15 to 20 year view, autonomous speed harmonization and sophisticated computer-directed intersection approaches are being explored by traffic futurists. Such technology, while offering significant traffic efficiencies, also come with potential threats of hacking and DDoS attacks capable of introducing chaos into the highway system**. The hacking of smart vehicles is a threat that DHS must explore and partner with other government entities, esp. the Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA), car manufacturers, providers and programmers of "smart car" technologies to prevent such nefarious activities.**

New categories of surface package delivery drones have also emerged and will continue to mature.[5] These small land-based vehicles, the size of a cooler, are motorized and have

[4] http://www.theverge.com/2016/10/25/13381246/otto-self-driving-truck-budweiser-first-shipment-uber
[5] http://www.toledoblade.com/Technology/2017/01/29/Delivery-robots-rolling-on-sidewalks-in-select-U-S-cities.html

directional, navigational, and communication capabilities. They are in advanced development by several companies to bridge the last mile between delivery truck and consumers using streets and sidewalks. Such delivery drones will radically enhance the process of bringing efficiencies to the marketplace. These too can be used for ill as well as good; capable of carrying explosives as they are delivering groceries. **Companies making these autonomous vehicles and delivery systems must be involved in the process of helping to keep their innovations safe. They, working with DHS and other Agencies, must ensure protections are in place to avoid illicit use or cause harm to others.**

Two Unmanned Aerial Vehicle (UAVs) drones penetrated the security perimeter around the White House and generated intense press coverage and government efforts to prevent future incursions.[6] These rather benign actions have been satirically referred to as "drunk droning" incidents. The surveillance benefits and risks associated with hobbyist and commercial drones with video data links have been considered in many forums.[7] Due to their availability, aerial drones can easily become significant enablers for other forms hostile activity, at minimum providing area surveillance and situational awareness only available to law enforcement and the military just a short time ago. But drones come in all shapes and sizes: militarized drones enact targeted killing; swarms of miniature drone may be deployed for various purposes, including creating self-propagating communication and surveillance networks; even an unsophisticated drone successfully gained aerial access in close enough proximity to where it was used by hackers to infect a "closed system" with computer viruses.[8] Other drones have been used to smuggle contraband into prisons and drugs across U.S. border fences. To date most, if not all, of the examples above featured human-controlled drones with some significant autonomous capabilities. A coordinated autonomous drone attack using chaff on electricity substations or explosives on gas and liquid fuel pipeline compressor stations might successfully be employed by terrorists in targeting and disrupting sections of our energy sector and cause cascading and devastating effects. **DHS must continue to partner with companies that manufacture technologies that can disrupt, disable, and control UAVs. In particular, DHS must work with the Department of Defense, other government agencies, and private corporations to develop the means to incapacitate rogue autonomous drones. They must ensure such technology is in place to protect high-value targets like government buildings, borders, prisons, and sensitive facilities. DHS must also work with the FAA and drone manufacturers to make sure they continue and expand placing certain no-fly areas off limits (which, for**

[6] http://www.cnn.com/2015/05/14/politics/white-house-drone-arrest/
[7] https://www.brookings.edu/blog/techtank/2014/11/18/drones-and-aerial-surveillance-the-opportunities-and-the-risks/
[8] https://www.engadget.com/2016/11/03/hackers-hijack-a-philips-hue-lights-with-a-drone/

example, includes the Greater Area of Washington, D.C., a no-fly zone for UAVs). This may involve mandating UAVs are only made available that include GPS geo-referenced data with denied areas restrictions programmed into all flight modes.

Despite the fact that flying everything from tacos to packages by autonomous UAVs has been the stated goal of companies like Amazon, Google, FedEx, and even the US Postal Service, the FAA has so far banned aerial drones for such commercial delivery use. The issue of delivery drones is one that is being heavily litigated with the possibility that a complete FAA ban will ultimately be amended. Around the world there has been exponential growth in the number of companies and technologies that are successfully delivering packages of all shapes and sizes by aerial drones**. DHS must enhance their working relationship with large UAV manufacturers and package companies to prevent their nefarious use and facilitate disaster logistics.**

The use of robots in factories will continue to mushroom as will the use of autonomous product movers that are now widely employed providing supply order fulfillment in distribution depots. Denial of service attacks could place America's advanced manufacturing sector at risk. Targeting production facilities that provide key components to "just-in-time" supply chains for manufacturers can introduce massive product shipping and manufacturing delays with the associated cascading effects. Companies manufacturing these devices should ensure that the control systems are not hackable: to prevent malefactors from stealing trade secrets or damaging manufacturing processes (i.e., making incomplete or unsafe products, including vehicles, tools, and consumer goods.) Even distributing a limited number of malfunctioning parts, sabotaging a small amount of products, or potentially endangering human workers in assembly lines could have an extraordinary, disastrous, and rippling effect on the economy. **The DHS should work with robotics manufacturers, factory owners, and distribution companies to put assessments in place, share best practices, work with companies to stimulate R+D, and prepare contingency plans for the reducing the risk of cyber sabotage and the possibility of widespread disruptive attacks.**

Autonomous technologies will also expand to residential use as well. New home, hotel, and hospital robotic aides must be designed with safety and software/ hardware integrity in mind so they cannot be misused to violate user's privacy or even injure users. This is especially important regarding devices developed to provide, monitor, and connect to medical devices that provide life support. These health devices may interact with a doctor's office or exchange personalized input from cognitive, reasoning systems like IBM Watson Health.[9] Such autonomous healthcare systems and robots might be attacked to cause harm to patients.

[9] https://www.ibm.com/watson/health/

Home dialysis machines may malfunction; insulin pumps could administer unsafe dosages; heart defibrillators and pacemakers could potentially not respond as designed, etc. Home cleaning robots with cameras with IoT (Internet of Things) interfaces can be hacked to allow electronic intruders to, for example, spy inside people's homes and/or capture mapping information these devices produce of their home working environment**. DHS must work with autonomous healthcare medical device manufacturers, FDA, NIST, home-helper robot companies, and others to ensure best safety practices are employed.**

Efforts to make massive container ships completely unmanned and "robotic" are underway where a vessel will be "commanded from an operating center on the other side of the world, where technicians are monitoring and controlling this vessel and others like it through a satellite data link—that is, when the ship isn't just controlling itself." [10] Manufacturers of such ships project they'll be able to carry larger loads with greater efficiency and lower wind resistance as these massive ships can be built eliminating crew quarters and deck houses. The manufacturers say these remote-controlled vessels will be significantly safer and less vulnerable to piracy, as they can be made without access to the controls and no humans will be aboard to take as hostages. Satellite controls, of course, can be hacked and remote vessels with extraordinary cargos can be targeted by thieves using other technological means of attack. **DHS S&T should work closely with the Coast Guard, Navy, and the various International Working Groups on Autonomous Vessels to ensure such vessels incorporate the best safeguards to avoid all possible dangers.**

Faced with greater success by U.S. authorities in interdicting illicit traffickers from South and Central America, using fast boats to smuggle drugs and other contraband in the homeland, smugglers have turned to using homemade low observable watercraft including submarines, to smuggle large quantities of drugs, contraband, or possibly illegal immigrants past our borders. New technology is being adapted to make unmanned autonomous submersible watercraft (for example, some disguised as logs) that can evade detection by submerging for significant distances. When discovered, semi-autonomous watercraft have been jettisoned from mother craft and sink below to depths, waiting for a signal from a mother ship or another craft to resurface when the coast is clear. Fully autonomous technology will likely follow submersible navigation and will enable smugglers to have completely waterproof craft self-navigate to predetermined destinations. **DHS must work with Coast Guard, U.S. Navy, and foreign allies to deter and detect drug-carrying submersible drones that smugglers or terrorist organizations are likely to harness as autonomous craft become mature.**

[10] "Autonomous Ships on the High Seas," Spectrum. IEEE.org, Feb 2017

We have identified just a few of the benefits and some of the potential consequences that may result from autonomous technology being used nefariously against targeted individuals, communities, and critical infrastructures, among others. In furtherance of the mission of the DHS, **critical risk analysis must begin immediately addressing the following four basic questions: "What can go wrong?"; "What is the probability?"; "What are the consequences?" and "What is the time frame?"11** The hidden nature of the misdirected, destructive misuse of autonomous technology against our society, and the associated challenges in their tracking and discovery, are enabled in part, due to our open society existing as a complex "system of systems."[12] Thus, an effective proactive counter response to this emergent risk requires thoughtful, analytical, committed, and ongoing systemic risk management plans by DHS to identify and assess threats to, and counter consequences from the misuse of, autonomous technology. **Risk management must be embedded in the formulation of public policy through proactive collaboration with local, national, international governments, corporate entities, and the public to identify and counter associated risks. This engagement is overdue and must become an urgent priority for DHS for analysis and action.**

Summary

In conclusion, Autonomous Technologies are coming rapidly or have already arrived. They bring many obvious benefits and efficiencies. They also expose us to many profound threats. **These threats need to be addressed before catastrophic consequences are unleashed. R&D and critical partnerships are needed. DHS S&T has an opportunity and a responsibility to assume a critical role in assuring our protection from the vulnerabilities these new technologies bring with them. This includes the challenge of insuring operational tests, evaluations, and certifications are performed of critical learning and Autonomous Systems. We need to actively address S&T's role in the Autonomous Technologies space and make programmatic decisions about what we want to invest in, advocate for, or simply monitor. Failure to do so will increase the risk of successful attacks on our Homeland.**

[11] Kaplan and Garrick, 1981; Kaplan, Haimes and Garrick, 2001
[12] Haimes, 2016, 2017