BROOKINGS

Paper | July 5, 2011

Cyber-Physical Attacks and Drone Strikes: The Next Homeland Security Threat

Most of the attention to the issue of cyberattacks is focused on the potential for the malicious use of electronic devices, computer systems and networks. But there is a closely related and much less widely appreciated threat in the form of physical attacks launched using cyber-physical systems. The U.S. National Science Foundation defines cyber-physical systems as "the tight conjoining of and coordination between computational and physical resources."[1] While the research community has focused on the many beneficial uses of cyber-physical systems including robotic surgery, search and rescue, healthcare monitoring, and high-performance manufacturing,[2] it is important to recognize that these platforms can be used for malicious purposes as well. In that respect, drones, also known as unmanned aerial vehicles or UAVs, constitute a significant potential security threat.

Drones are essentially flying – and sometimes armed – computers. The same advances in information technology that enable video-capable smartphones and wireless Internet-based movie delivery to laptop computers also make it possible to build smaller, less expensive, and more versatile drones. For example, the Wasp III microdrone used by the U.S. Air Force weighs under a pound and is less than a foot long, yet carries two on-board cameras and a GPS receiver and can fly at an altitude of 1000 feet.[3] In February 2011, California-based company AeroVironment announced the successful demonstration of the prototype Nano Hummingbird, a video-capable drone developed under DARPA funding that weighs only two-thirds of an ounce and has a wingspan of 6.5 inches.[4]

As drones become smaller and quieter, they become easier to move and launch, and harder to detect in operation. The prospect of foreign-owned drones not under U.S. control operating within the United States without our knowledge or permission is not purely theoretical. In fact, it has already happened.

In December 2010, a small Israeli-made drone operated by the Mexican federal police crashed in an El Paso, Texas backyard, causing no injuries.[5] That incident, which U.S. Customs and Border Protection Commissioner Alan Bersin later characterized as "an accident, no question about it,"[6] illustrated the uncomfortable reality that all of the analysis regarding the drone's origin, ownership, purpose, trajectory, and payload took place after the crash had occurred. Before the crash, U.S.

officials had not even been aware that drones were operating in the area.[7] Had the incursion been purposeful, targeted, and malicious as opposed to accidental, it appears highly unlikely that it would have been detected and stopped in advance of reaching its target.

To believe that drones will remain the exclusive province of responsible nations is to disregard the long history of weapons technology. It is only a matter of time before rogue groups or nations hostile to the United States are able to build or acquire their own drones and to use them to launch attacks on our soil or on our soldiers abroad.[8]

The national security threat posed by drones has been considered before. For example, Dennis Gromley of the Monterey Institute's Center for Nonproliferation Studies described the possible use of drones by terrorists in testimony before a House of Representatives subcommittee in 2004[9] and in a 2006 paper published through the Naval Postgraduate School.[10] Similar issues were also considered in a 2005 paper by Eugene Miasnikov of the Center for Arms Control, Energy and Environmental Studies at the Moscow Institute of Physics and Technology.[11]

In addition, the Government Accountability Office (GAO) released a report[12] in January 2004 addressing nonproliferation issues related to cruise missiles and drones from the standpoint of U.S. export control as well as multilateral export control through the Missile Technology Control Regime [13] and the Wassenaar Arrangement.[14] The drones of the early 2000s were often akin to cruise missiles in terms of size and weight, so in that era considering them jointly from the standpoint of nonproliferation in the manner of the 2004 GAO report was eminently reasonable.

Times have changed. In some respects today’s drones are more similar to smartphones than to cruise missiles. This is due in large part to several game-changing information technology advances that have occurred over the last several years. First, spurred in part by general consumer demand for high-quality commercial mobile video solutions for products such as smartphones and tablet computers, miniature cameras and computer chips able to acquire and process high-resolution, high-frame-rate video while consuming very little battery power have become inexpensive and widely available. Second, commercial wireless communications technologies and the associated standards and protocols have evolved to the point where wireless transmission of video has become routine.

These advances, in combination with innovations in drone airframe and propulsion system design, have made it possible to build very small, inexpensive drones, and to control them using an interface as simple as a laptop screen and computer mouse. Partly as a result of these changes, the U.S. military has increased its inventory of drones from under 50 drones a decade ago to about 7000 today.[15] Drones have transformed the way the U.S. military wages war, making it possible to gather unprecedented amounts of aerial imagery using nearly undetectable platforms, and to strike at targets without putting pilots at risk. However, these capabilities can be exploited by anyone with access to suitably equipped drones. That access will become dramatically easier as drones continue to become more numerous, smaller, cheaper, and more widely distributed in the global supply chain.

One source that a rogue group wishing to gain possession of one or more drones might look to is the U.S. military itself. The Pentagon is requesting almost $5 billion for drones next year, and as the Pentagon's chief weapons buyer recently stated, drones are "a growth market."[16] A recent study from the Virginia-based Teal Group predicts that global spending on drones will exceed $94 billion over the next ten years, with the United States accounting for nearly 70% of the procurement expenditures.[17] With thousands of drones flowing through a complex U.S. military procurement and deployment process in the coming years, there are multiple scenarios that would enable a U.S. military drone to end up in the wrong hands.

Some degree of loss in the distribution process is almost certain.[18] Somewhere, a box containing a drone will be left on a pallet, will fall off a truck, or will be left momentarily unattended and will disappear. Or, the box, when opened at its final destination, will be empty, with no practical way to determine when or where its contents were removed. Some drones will crash during missions and could be recovered by persons hostile to the U.S. In some cases the crash may leave the drone irreparably damaged, but in others the damage may be slight and easily repaired.

There is also the very real threat of an insider sale, as illustrated by the 2007 arrest of an ex-Navy officer for stealing and in some cases selling military equipment including machine guns, a shoulder-fired rocket launcher, and weapons-mounted infrared laser-aiming devices.[19]

The computer systems on U.S. military drones are presumably highly secured. But these are also easy to replace. A rogue group in possession of an airframe and propulsion system obtained from the U.S. military could use commercial off-the-shelf electronics components to replace the systems for acquiring video and for enabling ground-based control of the drone.

Alternatively, the group could attempt to buy a drone on the global market. As an El Paso Times newspaper article noted in December 2010, the drone model that crashed in El Paso is offered for sale on the Internet.[20] Increased demand for drones from the militaries of many different countries has led to larger numbers of drone suppliers, some based overseas and thus outside the direct reach of U.S. regulation, and some of those located in countries that are not members of the Missile Technology Control Regime or the Wassenaar Arrangement. For example, as noted in a July 4, 2011 Washington Post article,[21] China has a very active program to develop its drone design and manufacturing capabilities, as well as a desire to sell drones on the international market. China is not currently listed as a member state of the Missile Technology Control Regime[22] or of the Wassenaar arrangement.[23] An Air Force expert on the history of drones wrote in 2007 that there were over 50 countries engaged in the "development and employment" of drones,[24] and the Teal Group's 2011 World Unmanned Aerial Vehicle Systems report contains individual market forecasts for over 70 countries.[25] In short, the drone industry is large, complex, and global.

Solutions to the national security risk posed by drones in the wrong hands include 1) measures designed to make it as difficult as possible for rogue groups to obtain drones, and 2) steps aimed at stopping or minimizing the harm due to attempted drone attacks on American interests. The process of putting such solutions into place will require significant time and coordination among multiple U.S. Government and international entities, and should to be started well in advance of receiving indications of a possible impending attack.

Specific steps that can be taken include the following:

Stages in the U.S. drone supply chain with relatively weaker security and that would therefore be more vulnerable to robbery or theft can be identified and secured. In addition, information about the operational characteristics, computer hardware, software systems, and communications and networking environments associated with drone operation can be more highly compartmentalized.

Drone communications and control systems can be evaluated and modified as necessary to ensure that they are secure. As reported by the Wall Street Journal in 2009, in at least some instances U.S. Predator drones were transmitting video over an unprotected communications link, enabling insurgents in Iraq to intercept the video using inexpensive, off-the-shelf software.[26] Drone software systems can be designed so that they can be reprogrammed as needed post-deployment to implement appropriate encryption and anti-jamming methods.

U.S.-made drones can be designed to include chips or other electronics that would enable them to be tracked if they are lost. With appropriate design, these chips can be made very difficult to find without destroying or significantly damaging the drone in the process.

On-board computer systems on drones can be equipped with kill switches that could be tripped remotely if the drones go missing. Of course, it would also be important to ensure that the kill switches can only be accessed by a very limited group of trusted people. In addition, or in the alternative, in the manner of theft recovery software that is increasingly installed on laptop computers, the on-board computer systems on drones could include the ability to “phone home” upon activation, and to provide imagery and information related to location.

Electronics and other system components used in drones can be designed to include steganographic (hidden) information that would allow the original manufacturer and purchaser to be traced and identified. This could aid after-the-fact identification of the perpetrators of a drone-based attack, and could also provide a disincentive to carry out attacks in the first place.

Drones will be increasingly available internationally, potentially including on the international arms market. While that market is notoriously hard to monitor and even more difficult to regulate, the United States can use its engagement with other countries through organizations such as the Missile Technology Control Regime to continue to enhance global standards for drone export control, supply chain monitoring and integrity.

It should also be recognized that nonproliferation is a particularly complex issue with respect to small surveillance drones given their size and their legitimate uses for applications such as law enforcement. Another complicating factor is that many of the core information processing technologies used in today’s drones are similar or identical to solutions found in commonly available consumer electronics devices such as laptop computers and gaming platforms. Despite these challenges, domestic and multilateral export control laws and agreements can be reevaluated to assess their suitability given the changes in drone technologies in recent years. For example, current U.S. export control laws specifically address various aspects of drones, and, among other restrictions, specify a license requirement for non-military drones (as well as the associated systems, equipment, and components) having the “capability of controlled flight out of the direct visual range involving a human operator.”[27] Increased export control coverage with respect to the nature of the onboard processing on drones may also be warranted.

Sensitive U.S. government buildings and areas could be equipped with systems to detect and, if appropriate, electromagnetically or physically engage low-flying drones that would literally be under the radar of the systems deployed today that were built to track higher-altitude, passenger-bearing aircraft. The same advances in information technology that increase the risk that drones will end up in the wrong hands also make it much more practical to monitor the low-altitude airspace in sensitive areas and to effectively communicate and analyze the information gathered by such systems.

Physical defenses against drone attacks are more challenging both technologically and in terms of cost. However, there may be no choice but to develop them. An analog can be found in the Israeli Iron Dome system, which is designed to detect and destroy incoming rocket attacks. While that system has cost well over $1 billion dollars to date and is still only partially effective,[28] there are few people on the receiving end of those attacks who would argue against its development. Some of the technologies developed by the U.S. military and the major defense contractors for missile interception, if appropriately modified, would likely be highly effective in targeting drones.

Today we have the luxury of assuming that the sky above us is free of nearly invisible pilotless aircraft under the control of a hostile group and possibly carrying a payload that might do us harm. Continued advances in drone technology make it all but certain that in future years we will no longer have that luxury. Investing effort now to put in place the policies, systems, and procedures to address that inevitability can play a vital role in minimizing the chances of a successful drone attack on American interests.

[1] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286, retrieved July 3, 2011.

[2] Ibid.

[3] http://www2.afsoc.af.mil/library/factsheets/factsheet.asp?id=9114, retrieved July 3, 2011.

[4] http://www.avinc.com/resources/press_release/aerovironment_develops_worlds_first_fully_operational_life-size_hummingbird, retrieved July 4, 2011.

[5] http://www.elpasotimes.com/ci_17021017, retrieved July 3, 2011.

[6] Ibid.

[7] Ibid.

[8] Iran has a longstanding drone program. As long ago as 2004, Iran was believed to be supplying drones to Hezbollah that were then used to penetrate Israeli airspace. See http://articles.chicagotribune.com/2004-11-08/news/0411080154_1_lebanese-airspace-hezbollah-israel-and-iran, retrieved July 4, 2011.
[9] Testimony of Dennis M. Gormley before the Subcommittee on National Security, Emerging Threats, and International Affairs of the U.S. House of Representatives Committee on Government Reform, March 9, 2004, http://cns.miis.edu/testimony/testgorm.htm, retrieved July 3, 2011.
[10] Dennis M. Gormley, "Globalization and WMD Proliferation Networks: The Case of Unmanned Air Vehicles as Terrorist Weapons," Strategic Insights, Volume V, Issue 6, Center for Contemporary Conflict, Naval Postgraduate School, Monterey, California, July 2006, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA521376&Location=U2&doc=GetTRDoc.pdf, retrieved July 3, 2011.
[11] Eugene Miasnikov, "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects," Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology, 2005, http://www.armscontrol.ru/UAV/UAV-report.pdf, retrieved July 3, 2011. This report includes an appendix on pages 25-26 listing “Media Reports of Terrorist Attempts to Employ UAVs.”
[12] See http://www.gao.gov/products/GAO-04-175 (retrieved July 4, 2011) for a summary; a detailed report is available at http://www.gao.gov/new.items/d04175.pdf, retrieved July 4, 2011. Drones are referred to as “UAVs” in the report.
[13] See http://www.mtcr.info/english/index.html, retrieved July 4, 2011. “The Missile Technology Control Regime is an informal and voluntary association of countries which share the goals of non-proliferation of unmanned delivery systems capable of delivering weapons of mass destruction, and which seek to coordinate national export licensing efforts aimed at preventing their proliferation.” There are currently 34 countries participating in the MTCR, including the United States. The MTCR “Equipment, Software, and Technology Annex” is available at http://www.mtcr.info/english/annex.html.
[14] The Wassenaar Arrangement currently has about 40 member states including the United States, and promotes “transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies.” See http://www.wassenaar.org/introduction/index.html, retrieved July 4, 2011. UAVs are addressed in the December 2010 Wassenaar Arrangement Control List under Category 9,
“Aerospace and Propulsion,” available at http://www.wassenaar.org/controllists/index.html.
[15] http://www.nytimes.com/2011/06/20/world/20drones.html, retrieved July 2, 2011.
[16] Ibid.
[17] http://tealgroup.com/index.php?option=com_content&view=article&id=74, retrieved July 4, 2011
[18] Procedures to track and account for military equipment, including weapons, are not always followed. For example, a November 2007 report from the Pentagon Inspector General identified thousands of unaccounted for weapons (though not drones) that passed through the 810,000 square foot warehouse complex at Abu Ghraib in Iraq, including rocket-propelled grenade launchers and machine guns. See http://www.cbsnews.com/htdocs/pdf/IG_Report_Security_Forces_Fund.pdf, retrieved July 3, 2011, pages 9 and 32.
[19] http://www.navytimes.com/news/2008/10/navy_lasertheft_102308/, retrieved July 4, 2011.
[20] http://www.elpasotimes.com/ci_16875462, retrieved July 3, 2011.
[21] http://www.washingtonpost.com/world/national-security/global-race-on-to-match-us-drone-capabilities/2011/06/30/gHQACWdmxH_story.html, retrieved July 4, 2011.
[22] http://www.mtcr.info/english/partners.html, retrieved July 4, 2011.
[23] http://www.wassenaar.org/participants/index.html, retrieved July 4, 2011.
[24] Lt. Kendra L.B. Cook, “The Silent Force Multiplier: The History and Role of UAVs in Warfare,” 2007 IEEE Aerospace Conference, pp. 1-7, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4161584, retrieved July 3, 2011.

[25] http://tealgroup.com/index.php?option=com_docman&task=doc_download&gid=395, retrieved July 4, 2011.

[26] http://online.wsj.com/article/SB126102247889095011.html, retrieved July 4, 2011

[27] See, for example, category 9 of the U.S. Commerce Control List, which is Part 774 of the Export Administration Regulations Database, available at http://www.gpo.gov/bis/ear/ear_data.html.

[28] http://www.guardian.co.uk/world/2011/apr/11/israel-iron-dome-anti-missile-system, retrieved July 2, 2011.

AUTHORS

John Villasenor
Nonresident Senior Fellow
Governance Studies, Center for Technology Innovation

RELATED INITIATIVES

CENTER FOR TECHNOLOGY INNOVATION

GOVERNANCE STUDIES

RELATED TOPICS

Defense

Homeland Security

Military Technology

Global Governance

Cybersecurity

Information Technology

Terrorism

U.S. Military Affairs

Technology

Drones