The Coming Robot Crime Wave

Noel Sharkey, Marc Goodman, and Nick Ross

Rapid advances in robotics technology for the battlefield and policing could promote a new breed of copycat "garden shed" robot criminals.

A miniature helicopter enters your workplace through an open window. It avoids alarms and security cameras as it navigates its way to your boss's office. It removes a flash drive from her desk and deposits a substitute—maybe bearing a potent virus—so the crime goes undetected.

This would have been science fiction until recently but now it is part of the Sixth International Aerial Robotics Competition, held at the University of Puerto Rico in 2010. While this is a wonderful challenge, it also serves as a forceful warning of crime's coming robotization.

Crime ebbs and flows according to available temptations, provocations, and opportunities. We must recognize that any human progress can be a power for harm as well as good and that we all must think through how actions could be used or abused. This consideration was not made for shops and vehicles and later we had to retrofit solutions. The pattern repeated when we filled our homes and pockets with expensive gadgets and had to install locks or learn to enter codes.

Cyber attacks

Predicting something like an inevitable robot crime wave might sound dramatic, but we've already witnessed massive international developments in service robotics in the past decade, with the greatest market share in military applications ranging from bomb disposal to surveillance to armed aerial and ground robots (The Profession, Nov. 2007, pp. 106-108). Much of this technology is returning to the civilian world through policing and border control. Micro-helicopters are being deployed for surveillance in the UK, with the plan to extend this activity to fixed-wing planes. Predator drones already patrol the US border with Mexico, while Canada and several more counties are seeking FAA approval for similar patrols.

Ground robots are being adapted for policing tasks such as hostage rescue, and arming them is clearly on the agenda. iRobot and TASER International, the "stun gun" company, announced a strategic alliance in 2007 (The Profession, Aug. 2009, pp. 101-104).

The human touch

Computing professionals know that the real and immediate danger is not that machines have a will of their own (the scenario beloved by sci-fi writers), but that unauthorized people do. Computers are only secure until someone works out how to hack them. We already have problems with computers being hijacked to work without their owners' consent, usually for criminal purposes. Wireless and remote control systems provide more opportunities for hacking, so it could just be a matter of time before an armed police robot turns against officers, before drones are piloted into buildings, or before robots are directed into a street to block traffic.

Another potent danger comes from standardization that, while highly desirable in many ways, exposes whole systems to harm. For example, the adoption of a universal robot operating system could pave the way for large-scale cyber attacks, as is the case with PC operating systems. There are always loopholes and backdoors in programs; we can fix them for the next time, but given what we know about computing vulnerabilities, and given our experience of how waves of conventional crime result from insufficient forethought, it would be reckless to worry about robot crime only after the genie leaves the bottle. As with town planning and physical design of goods, robot developers should "think thief." Planning against crime must be an integral part of the design process.

Continued on page 114

 Published by the IEEE Computer Society

Continued from page 116

The "Bum Bot" vigilante robot by Rufus O. Terrill protecting O'Terrill's Bar, Atlanta, GA.

Skeletron, the rope climbing robot, turns to a life of crime (Robot and photo by Ray Tait).

Flying in the face of the law

Building robots is 80 percent cheaper now than it was 20 years ago, and all of the required components and sensors are readily available on the Internet. We don't need to be skilled engineers or electronics experts anymore. The engineer's job is to build robust and safe machines, but this isn't required for a disposable crimebot. With less concern for safety, crude copies of mechanized police and military devices can be made relatively easily. YouTube is replete with hobbyists showing mechanisms that perform elaborate tasks such as tracking and shooting people with paint balls or water pistols—a pastime ideal for terrorist adaptation.

Tomorrow's machines will be far more sophisticated than today's, but cheap off-the-shelf platforms already await modification for criminal purposes. A craft like the Parrot iPhone-controlled helicopter (http://bit.ly/a65Cor) could be fitted with many widely available technologies, including audio and video feeds, GPS tracking, and GSM controls. It could then be used for a wide variety of nefarious activities, including counter-surveillance of law enforcement, remote voyeurism, "casing" a location by obtaining high-resolution video images, intellectual property theft, electronic bugging, and competitive intelligence gathering. Terrorist attacks, bullying, assault, vandalism, and vigilantism are all possible.

Most conventional crime flourishes because of ill-considered weaknesses in mainstream goods and services. The anonymity permitted through the Internet, for example, seems to have encouraged many people to become criminals who wouldn't otherwise have been so antisocial, including teenagers working from their bedrooms. Hacking is the prime example, opening as it does so many opportunities for vandalism and fraud. Likewise, the growing availability of robotics knowledge and components could promote a new breed of "garden shed" robot criminals.

Grounds for concern

In 2008, Rufus Terrill, a bar owner in Atlanta, Georgia, decided to police his own premises by building a robust and remotely controlled "*Bum Bot*" to patrol the area around his bar at night (http://bit.ly/bVjAiZ). He would stand on a street corner with a radio controller and use a camera on his four-foot, 300-pound machine to look for drug dealers and vagrants, then shout through an onboard walkie-talkie to urge them to move on. If they disobeyed or threw objects at the robot, he would open fire with a water cannon. Whether this is crime fighting or criminal activity, it shows how easy building armed machines can be.

Alternatively, drug cartels could adapt such devices to be drug runners and mobile vending machines for robotic dealers, who would provide a fix if offered the correct asking price. Unlike regular vending machines, such devices could be defensive and possibly lethal. Given 360-degree vision, the bots, under imminent threat of capture, could automatically destroy the internal stash. In time, robots could even be used to assist in bank robberies, street holdups, and heists of high-value delivery trucks, perhaps with a combination of ground robot assailants and aerial lookouts. Moreover, robots and related technology, such as exoskeleton suits, offer physical strength vastly superior to that of human beings. As such, they could facilitate crimes such as assault, rape, or murder.

The more sophisticated robots become, the greater the danger of their being stolen or adapted for misuse. Miniaturization will facilitate a wide range of offenses such as sending machines through letter

boxes, cat flaps, or partially open windows to search for keys or to neutralize intruder alarms. Most existing alarms use passive infrared detectors that wouldn't be able to detect a cold-blooded mechanized intruder, meaning alarm companies must think through such implications sooner rather than later.

These new technologies also raise the risk of invading privacy on a gigantic scale. As ever more robots proliferate in our homes and workplaces, the more tempting it will be to use them to record intimate activities. Many household security robots are designed for simple Internet operation, which makes them insecure. Will your humble Roomba vacuum cleaner be used to transmit naked videos of you?

Narco submarines

Major criminal organizations such as drug cartels don't need to rely on cheap home engineering. Discoveries of submarines designed to carry tons of narcotics have been occurring since 1988. With 10 tons of cocaine netting $200 million, $2 million for a submarine would repay the robot's cost many times over in one voyage. The drug cartels clearly have the money to adapt their technology to keep ahead of enforcement agencies.

Once the exclusive and secretive preserve of the military, this technology is becoming commonplace in civilian applications, with marine robots a prime example. So far, they've been used to locate the *Titanic*, investigate ice caps, build deep sea oil rigs, repair undersea cables, and mitigate environmental catastrophes such as the recent Deepwater Horizon explosion in the Gulf of Mexico.

In 2010, US officials secured the first convictions for remote-controlled drug smuggling when they imprisoned three men for building and selling drug subs (http://bit.ly/b8Qawc). At the Tampa hearing, attorney Joseph K. Ruddy reported that these remote-controlled submarines were up to 40 feet long and could carry 1,800 kilograms of cocaine 1,000 miles without refueling. The effectiveness of these submarines in avoiding detection is clear, given that none have ever been seized. We only hear about the criminals' failures, so there could be none, dozens, or hundreds of these machines in use.

The latest autonomous and semi-autonomous submarine capabilities pose a greater concern. They can act on their own when required, employ programmed avoidance routines to thwart authorities, be fitted with sensors to send signals to the operator when the payload is delivered or the craft attacked, and carry self-destruct features to destroy incriminating evidence. Each year, the technology improves, gets cheaper, and becomes more widely accessible. For example, students at Washington University built an autonomous submarine called Deep Glider that can reach depths of nearly 9,000 feet, which would make it extremely difficult for customs agents to detect. Although the Washington machine couldn't carry a heavy payload, it demonstrates future criminal possibilities. Moreover, we can assume that submarines won't be used for drugs alone. They can transport any illegal objects and could certainly be useful to terrorist organizations. Even human trafficking is possible because it would be less risky to the smugglers: only the people being trafficked could be detained.

The growing availability of robotics knowledge and components will promote a new breed of "garden shed" robot criminals.

Robots will be used for crimes because they offer two elements that have always promoted crime: temptation and opportunity. The rewards are high, the barriers to entry rapidly disappearing, and the risk of apprehension significantly decreasing. Catching a robot doesn't catch the perpetrator, so a new form of forensic science must be created.

Robots don't leave fingerprints or DNA, so police should consider building information databases to match and trace robot crime just as they do guns and ammunition. Meanwhile, engineers should seek ways to incorporate telltale clues into software and components to assist forensic analyses.

The creativity of the human mind is difficult to predict but we do know that any vulnerabilities will be exploited for ill as well as good. The new crime wave might be 10 years away or 20 or more, but we should have no doubt it's coming. Unless we plan to sleepwalk through disaster, we need to act quickly and decisively to head off a pandemic of robot crime.

Noel Sharkey *is a professor of robotics and artificial intelligence, a professor of public engagement, and a Leverhulme Research Fellow at the University of Sheffield, UK. Contact him at noel@dcs.shef.ac.uk.*

Marc Goodman *is the founder of FutureCrimes.com, a visiting researcher at the University College Dublin's Centre for Computer Crime Investigation, and a senior advisor to Interpol. He previously served as the officer-in-charge of the Los Angeles Police Department's Internet Unit. Contact him at goodman@cybercrime-institute.com.*

Nick Ross *is a broadcaster who founded the UCL Jill Dando Institute of Crime Science, where he is a visiting professor. He's a fellow of the Academy of Experimental Criminologists and a trustee of Sense About Science. Contact him at nick@nickross.com.*