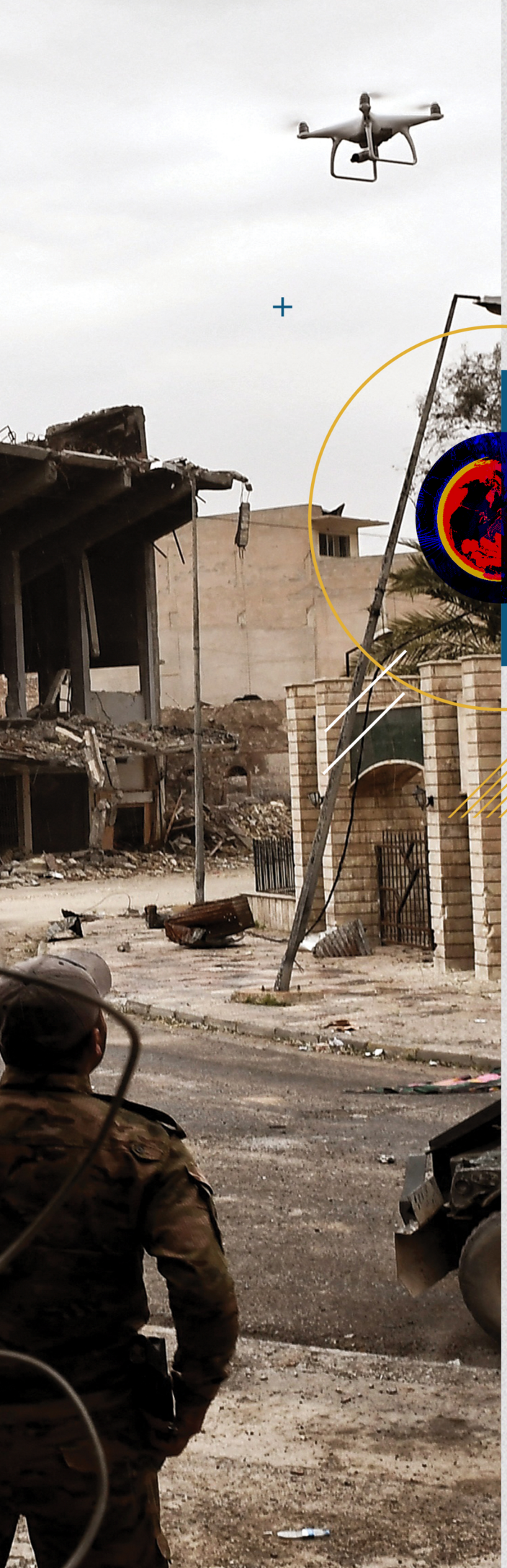


TRANSREGIONAL THREATS JOURNAL

ISSUE 09

KILLER DRONES: HOW COMMERCIAL DRONES ARE CHANGING THE INTERNATIONAL SECURITY ENVIRONMENT

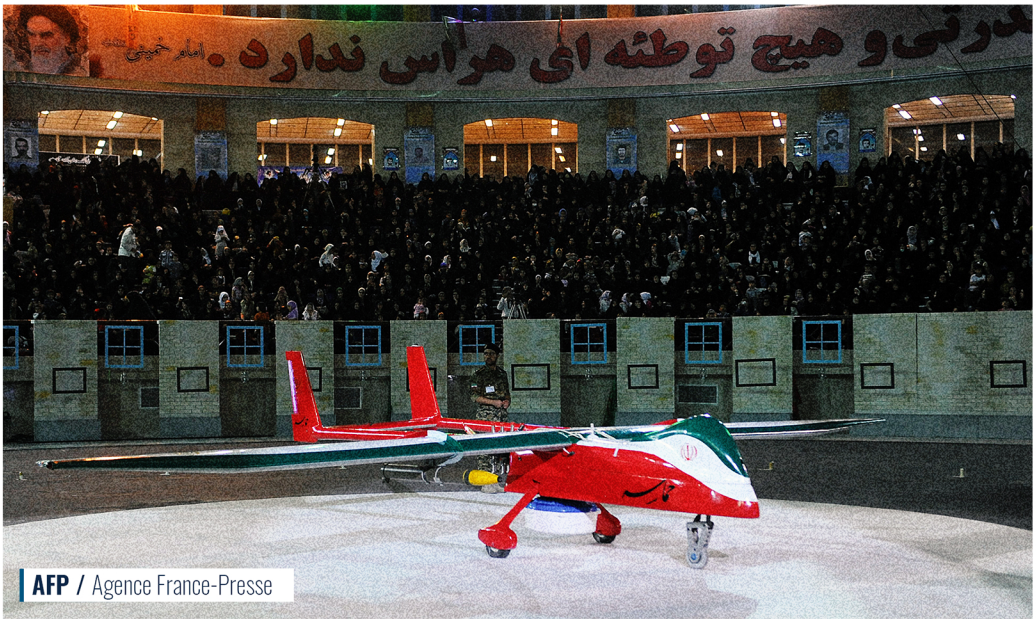
By Bill Edwards

June 2022

CENTER FOR A SECURE FREE SOCIETY

Advancing **freedom** and **security worldwide**

BOTTOM LINE UP FRONT:



1. **As of 2022, there are more than half a million drones in private hands in the US alone and the global market from drone sales is expected to grow to reach $43 billion in 2024.**

2. **The abuse of commercial drones can affect the security of critical infrastructure**, transportation, and industrial, commercial, and personal data.

3. **Even more concerning, drone technology is now being used in various conflicts around the world**, deploying drones for surveillance, drug trafficking, and to launch armed attacks by non-state actors.

4. **Staying informed about current advances in drone technology and how it is being used in conflicts around the globe is critical in this new security and business environment.** This includes policymakers developing supportive measurements such as task forces on drones, more specific research on capabilities, and vulnerability assessments on critical infrastructure.

AN ADVISOR TO UKRAINIAN PRESIDENT VOLODYMYR ZELENSKY

shared an anecdote that Ukrainian soldiers were using commercial drones disguised as equipment from the fictional Skynet, the artificial intelligence network shown in the Terminator film series.[1]

In essence, the *"terminator drones"* would surveil and scare Russian troops prompting them to retreat to their base allowing Ukraine's military to pinpoint the precise location of the Russian military – and attack them.

TRANSREGIONAL THREATS JOURNAL

This creative use of disguised commercial drones is just a glimpse of how drones can, and will, be used in modern warfare. Although the use of drones in conflicts is nothing new, the war in Ukraine is the first time a government asked private citizens to deploy their recreational drones to support a country's defense.[2]

With more than 27-years of experience with intelligence and military operations in the U.S. government and Special Operations community, I have seen the benefits that technology brings to the battlefield – but have also seen the associated threats. Drones provide no better example of a technology that has great benefits for society but even greater challenges.

To keep critical assets and people safe, U.S. policymakers must focus on developing policies on how to deal with drones from defensive and offensive security standpoints. We need to have the capability to action the threat without disrupting commercial activities or cause a scenario for collateral damage. Particularly in areas where the nature of the target of a potential drone attack is critical for societal use, such as critical infrastructure or supply chains. This is especially the case as drones become more commercial and common in day-to-day activities.

Abuse of Commercial Drones

As of 2022, there are more than half a million drones in private hands in the United States alone.[3] The global market on drones is expected to grow at a compound annual growth rate of 20.5 percent to reach nearly $43 billion in 2024 from drone sales.[4]

PHOTO: UNSPLASH / Diana Măceşanu

This is good news for technology enthusiasts and entrepreneurs but, unfortunately, is also drastically reshaping the tools and methods of illicit actors, and allowing them to enhance their capabilities against military and law enforcement measures.

Drones have become the tool of choice and commonplace in visible attacks on critical infrastructure. Look no further than a recent event at a Pennsylvania electric substation to demonstrate that commercial drones can be used to target key facilities in the United States' homeland.[5] The ripple effects from various conflicts have shown that drone technology and the nefarious uses of drones (bombings, suicide attacks, surveillance) are now making their way from combat zones to the private sector in the United States and other countries. More importantly, our airspace controls from a legal and regulatory perspective are being outpaced by the change in the environment from the use of commercial drones. Complicating issues still remain unsolved concerning unmanned traffic management (UTM) and in the future urban air mobility (UAM)---think of this as a way to move people and goods in the unmanned environment.

Commercial drones in today's market can be outfitted with small computing devices called raspberry pi and execute spoofing techniques to exploit unsecured networks and devices.[6] In basic terms, the drone makes you believe you are on your network, but you are communicating through the drone's onboard computer as it takes over your connection. Moreover, local networks are not the only target; these platforms can also attack your smart devices through Wi-Fi and Bluetooth connections. Your data is easily accessed by a drone simply following you down the street.

As the world looks to address the growing interest in commercial drone usage as an everyday tool and a societal norm, there should be an emphasis put on these platforms and how they affect the security of critical infrastructure, transportation, industrial, commercial, and personal data.

New Technology, New Threat

When I was stationed in Iraq in the U.S. Army from 2010 to 2011, I witnessed both the benefits and dangers of drones as a commander with Unmanned Aircraft Systems (UAS) capabilities and then later as a theater director of intelligence.

In the latter role, I saw firsthand how drones can be used to carry weapons weighing up to 15 pounds on commercial UAS platforms and much heavier weapons on other platforms designed for military use.

Years later, in 2016, the U.S. admitted a lapse in tactical superiority of the airspace during the battle of Mosul against the Islamic State in Iraq and Syria (ISIS). This shows how drones are leveling the playing field between violent[7] non-state actors and the militaries tasked with combatting them. Look no further than the war in Ukraine to see commercial and military-grade drones working together to bring a sense of air parity to Ukrainian forces.

From kinetic attacks to cyberattacks, intellectual property theft, to spying and assassinations. The list goes on, perhaps limited only by the imagination of the nefarious non-state actor or a rogue nation-state Terrorist and criminal organizations have developed, conducted, and promoted weaponized drone attacks in conflict zones, and even promulgated the technology for use outside of these areas.
The malicious use of these platforms by criminals and terrorists is an inevitable fact and can no longer be pushed[8] aside.

COMING TO A BORDER NEAR YOU

In September 2019, the Colombian Army announced it found two Syma drones between the municipalities of Pasto and Tumaco, in Nariño, along the border of Colombia and Ecuador.[9]

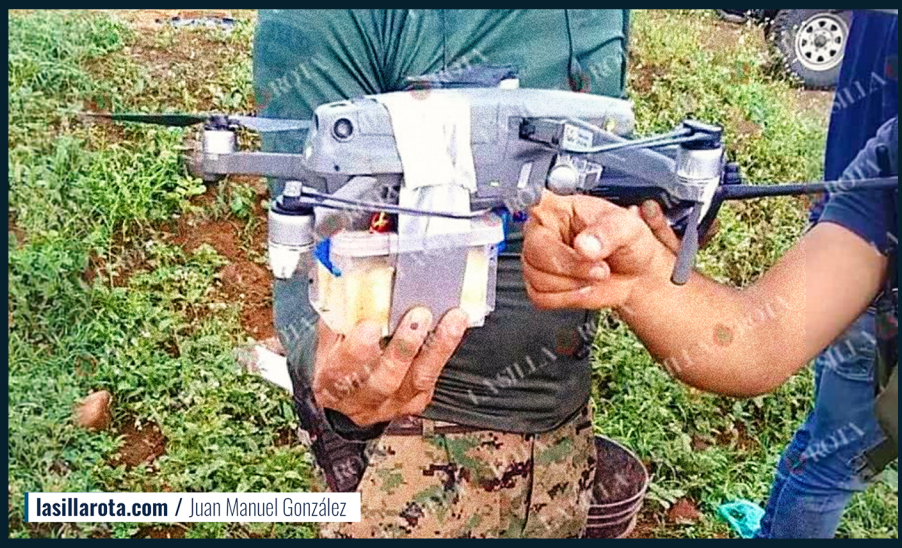
A subsequent Colombian Army press release stated the owner of the drones was the Oliver Sinisterra Front (Frente Oliver Sinisterra - FOS), dissidents of the Revolutionary Armed Forces of Colombia (FARC), an armed non-state actor once designated as a terrorist group by the United States.[10] That same month, Colombian police reported seeing drones flying over the Saravena, Neiva, San Jose del Guaviare, and Tumaco cities of Colombia, along the border with Ecuador.

Some analysts suggested that these drones belonged to the National Liberation Army (ELN), another recognized narco-terrorist group operating in Colombia and Venezuela.[11]

FFMM / Colombia

Drone usage by criminal groups has been reported before for surveillance, but this was the first time in Colombia that drones were found for use as weapons. In 2021, the Colombian military stated that FARC dissidents could be planning drone attacks against public security forces in the Tibú municipality in the northeast of the country on the border with Venezuela.[12]

Colombia is just one country where drones are quickly becoming a game-changer for public security forces combatting transnational organized crime and terrorism. A more pressing example is in Michoacan, a Mexican state with the third-highest number of murders and where rival cartels are using drones to transport small amounts of drugs and on occasion, to launch attacks.



In mid-January, a video recorded by a drone controlled by the Jalisco New Generation Cartel (Cartel Jalisco Nuevas Generaciones–CJNG) went viral. In the footage, the drone is seen to drop several bombs on Tepalcatepec, a municipality in Michoacán that has been hard hit by narco-violence.[13] This type of drone attack has psychological effects on the Mexican population who begin to perceive the drug cartels as more powerful than the public security forces tasked with protecting them.

This means that as drone technology continues to develop, it presents an ever-growing challenge for policymakers and security professionals worldwide. The concern increases as the targets of drone attacks become more strategic, such as critical infrastructure and/or supply chains, and as drones become more readily available on the commercial market. There is no simple solution as the range of threats from drones is wide, but there are various risk mitigation measures that can be taken and tailored to address specific security situations involving drone technology.

RISK MITIGATION

Staying informed about current advances in drone technology and how it is being used in different conflicts across the globe is critical in this new security and business environment.

The good news is there are operational security measures that can be taken to mitigate the growing risks presented by commercial drones.

Individually, for instance, one can combat the threat posed by commercial drones by ensuring that every network or connection accessed is secure. That would mean staying clear of public Wi-Fi that is accessible without a password. If you are a business, it is advised that you secure your employee networks, remember to change passwords daily, and monitor your network for nefarious or suspicious activity. Additionally, dedicating a secure space and RF shielding for very sensitive meetings is another way to layer your defense against misuse of drone technology.

There are also new advanced software and modeling tools that can be used to identify vulnerabilities in a specific airspace.

Technological mitigation platforms – like a drone detection and monitoring system, mass communication notification system, physical air-space observation posts, and communication systems – are necessary, as is an early warning system that allows for the time and space necessary for a quick reaction.

These measures are often nested within a **Drone Vulnerability Risk Assessment (DVRA)**, a Drone Detection, and Response (DDR) plan, and Drone Emergency Response Plan (DERP),[14] which establish and confirm standard operating procedures and emergency response actions, bringing in law enforcement, private security, medical services, and hazardous material experts when necessary.

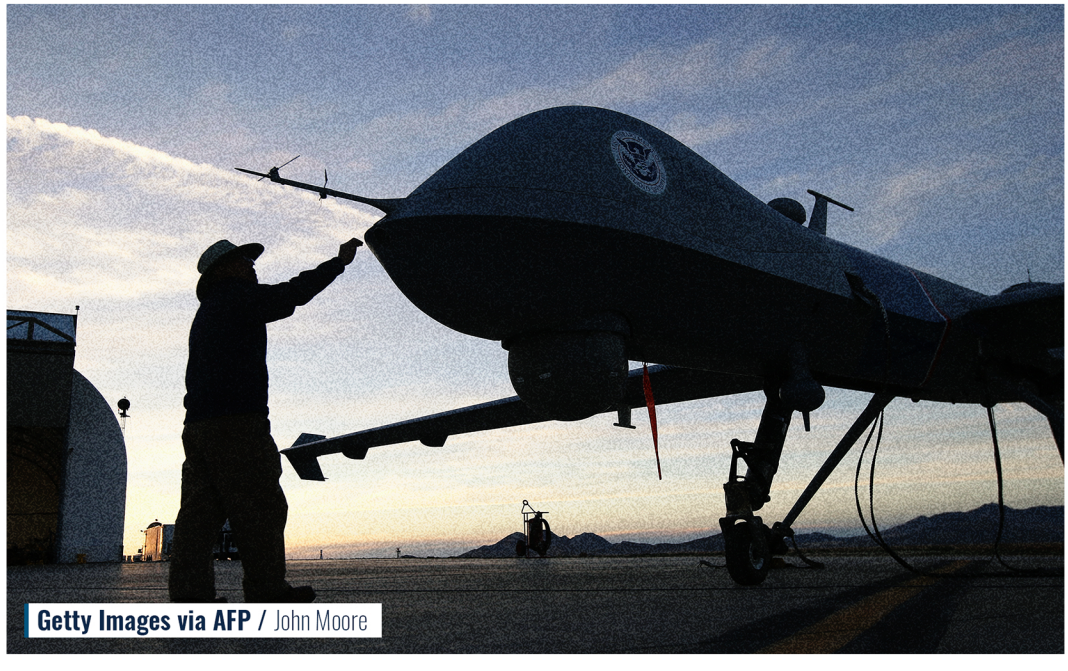
More unsettling, however, are concerns for critical infrastructure, supply chains, and data centers.

The growing use, from personal devices to complex business operations, of cloud storage is taking over as the world's data storage technology of choice. On-premise storage of data is becoming a technique of the past. This makes cloud storage within critical infrastructure and supply chains a possible vulnerability for electronic espionage and intellectual property theft via drone technology.

That is why it’s imperative that policymakers, security professionals, and intelligence personnel stay current with the technology, understand the capabilities, and proactively work with all key stakeholders to address the quickly evolving pace of technological advancement and access of commercial drones in public space.

Policy Solutions

From Ukraine to Colombia to our U.S. southern border, the use of drones is changing and extending the battlefield in modern warfare. Drones now have access where access control is almost obsolete.



Getty Images via AFP / John Moore

The concept of detection and monitoring is only beginning to take shape in environments where laws and regulations haven't kept pace with technological growth.

These are steps that policymakers can take to mitigate the growing risks associated with commercial drones, and to protect critical infrastructure, transportation, supply chains, and public spaces from unauthorized drone activity:

1

Policymakers need to mandate that all entities associated with critical infrastructure conduct a targeted drone security and vulnerability assessment (DVRA) focusing on access to the facility, vessel, platform, and public space.[15]

This will include identifying and prioritizing vulnerabilities that require protection and expanding outward from those areas, establishing no-fly boundaries that should be heavily monitored by technical solutions that have the capability for offensive measures if warranted. This will require identifying the resources – including capital, personnel, systems, and outside experts – to implement the infrastructure and expertise required for the detection and monitoring of threats. In addition, stakeholder engagement on many levels, including leveraging security consultants to advise and assist policymakers from a practitioner level, is necessary.

2

Policymakers should research to better understand product lines, specifications, and capabilities associated with commercial drones which will make establishing control measures around critical infrastructure, transportation, and public venues simpler.

The market is controlled by three companies that supply nearly 100 percent of drones sold globally. However, the fourth major producer of commercial drones is the hobbyist, and in this area of production, extending similar controls is nearly impossible. Careful and creative thought is needed to address the fourth dimension of drone use in public space.

3

Policymakers, and particularly the U.S. Congress, should create a standing Task Force on Commercial Drones.

This task force should be composed of relevant federal agencies, private sector practitioner, academic, and subject matter experts, to create a holistic integrated approach to ensuring resources are allocated in the most effective manner. A true public/private partnership that helps define the division of labor between federal, state, local and tribal governments that regulate commercial drone use and protect privacy concerns while supporting safe regulation and coordination of airspace.[16]

TRANSREGIONAL
THREATS JOURNAL

In the end, there needs to be a concerted effort from policymakers to take drone technology seriously and develop supportive measures for internal and external entities associated with protecting and securing critical infrastructure, transportation, and public space.

Eliminate the stovepipes and one-off efforts. Drone technology is on a clear glide path to pick up even more momentum as a norm in everyday life. This has the potential to help improve market efficiency, but if left unattended, it also has the potential to disrupt life systems, free flow of goods, services, and labor, and impede our ability to safely participate in public events. The future is now-- there is no time to waste.

Bill Edwards

Colonel (ret.) Bill Edwards joined Calibre Engineering in December 2021 as President of the firm. Bill retired from the military in 2017 and led Thornton Tomasetti's security consulting group as a Principal from 2017 – 2021. He offers over 34 years of expertise in operational/technical security, counter terrorism, counter-intelligence, surveillance and counter-surveillance.

He served as the Director of Intelligence for Theater Special Operations Command-North, a position that required extensive collaboration and partnering across the U.S. whole of government security enterprise.

He specifically designed a cohesive and collaborative counter-terrorism network with Department of Defense, Law Enforcement, and Inter-Agency partners while simultaneously bridging strong relationships with coalition partners to further extend his security reach in an effort to protect the homeland.

Col. Edwards also brings extensive experience in operational/technical security from his combat deployments to Iraq, where he commanded large bases in Al Anbar, Dhi Qar, and Basra Provinces, focusing primarily on operations and security. During this time period, he oversaw the planning and execution of all base infrastructure to include the implementation and operation of U.S. base security.

He also planned and designed multiple levels of security improvements to combat threat. Bill recently published a book titled Inside Abu Ghraib: Memoirs of Two U.S. Military Intelligence Officers. The book is about leading through adversity and the military family during combat operations. Bill also teaches leadership, strategic communications, and negotiations to senior Air Force officers through the Air Force War College.

Bill Edwards is an ASIS International board certified CPP, PSP, and PCI. He is also certified as a CPTED Professional (CPD), Identity Management Professional (CIMP), a FEMA Level 1 Continuity Planner and a licensed FAA Part 107 Drone Operator.

NOTES

1. Aila Slisco. *"Ukraine Army Is Using 'Terminator Drones' to 'Scare Russians' Into Retreat,"* Newsweek, April 7, 2022: www.newsweek.com/ukraine-army-using-terminator-drones-scare-russians-retreat-1696192

2. Zak Kallenborn. *"Send in the Quadcopters: Arm Ukrainian Citizens with Simple Drones,"* Defense One, March 3, 2022: www.defenseone.com/ideas/2022/03/send-quadcopters-arm-ukrainian-citizens-simple-drones/362730/

3. *"Drones by the Numbers,"* Federal Aviation Administration, May 2, 2022: www.faa.gov/uas/resources/by_the_numbers/

4. *"The Drone Market: Insights from Customers and Providers,"* Comptia, June 2019: www.connect.comptia.org/content/research/drone-industry-trends-analysis

5. Sean Lyngaas. *"Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure,' according to federal law enforcement bulletin,"* CNN, November 4, 2021: www.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation/index.html

6. Erica Fink. *"This drone can steal what's on your phone,"* CNN Business, March 20, 2014: www.money.cnn.com/2014/03/20/technology/security/drone-phone/

7. Kerry Chávez and Dr. Ori Swed. *"Off the Shelf: The Violent Nonstate Actor Drone Threat,"* Air & Space Power Journal, Fall 2020: www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F-Chavez_Swed.pdf

8. Karen Allen. *"Drones and Violent Nonstate Actors in Africa,"* Africa Center for Strategic Studies, August 6, 2021: www.africacenter.org/spotlight/drones-and-violent-nonstate-actors-in-africa/

9. Maria Alejandra Navarrete. *"Drones Pose New Threat on Colombia's Pacific Coast,"* Insight Crime, September 25, 2019 www.insightcrime.org/news/brief/drones-emerge-new-weapon-war-colombia-pacific/

NOTES

10. *"Neutralizados y destruidos dos drones cargados de explosivos,"* La Seguridad es de Todos, September 19, 2019: www.ejercito.mil.co/index.php?idcategoria=467681

11. *"Narcos, disidencias y ELN estarían utilizando drones para espiar a la fuerza pública,"* Blu Radio, September 19, 2019: www.bluradio.com/nacion/narcos-disidencias-y-eln-estarian-utilizando-drones-para-espiar-a-la-fuerza-publica

12. *"Dissident FARC group claims responsibility for attack against Colombian President Duque,"* MercoPress, July 26, 2021: www.en.mercopress.com/2021/07/26/dissident-farc-group-claims-responsibility-for-attack-against-colombian-president-duque

13. Alejandro Santos Cid. *"Drones: The latest weapon (and status symbol) of Mexico's cartels,"* El País, February 1, 2022: www.english.elpais.com/usa/2022-02-01/drones-the-latest-weapon-of-mexicos-cartels.html

14. Ibid

15. Bill Edwards. *"Drone Emergency Response: A Planning System for Critical Infrastructure,"* The Infragard Journal, Volume 3, Issue 1, Winter 2020: www.infragardnational.org/wp-content/uploads/2020/02/Article2pdf.pdf

16. Mark E. McKinnon. *"GAO Weighs in on Drones,"* Plane-ly Spoken, September 17, 2020: www.plane-lyspoken.foxrothschild.com/

Advancing **freedom**
and **security worldwide**

Center for a Secure Free Society
655 15th Street, NW, Suite 800 Washington, D.C. 20005
+1 (202) 909-1107 info@securefreesociety.org

WWW.SECUREFREESOCIETY.ORG