Emergence of Technological Threats and Opportunities for Nuclear Security in the Digital Age

YEVHEN KALINICHENKO (UKRAINE)

The development of science, technology and means of production creates both new opportunities and new threats to nuclear security.

Drone Threat

For example, the availability and using of unmanned aircrafts systems (UAS) or drones have increased significantly in recent years. Today, drones are available in sizes ranging from a matchbox to those that can lift an adult. Their capabilities are amazing. They can be incredibly maneuverable, slipping into small windows at full speed and navigating inside buildings [1]; act autonomously [2] according to a predetermined plan. Some drones can remain in the air even after a partial loss of rotors, and act in coordination with large groups of other drones [3], [4]. Their scope is huge: aerial shooting, inspections, agriculture, searches, rescues, firefights, cargo delivery and many more. Naturally, so capable and easily accessible technology is already widely used by smugglers [5], terrorists and in modern conflicts for aerial reconnaissance, artillery fire adjustment, sabotage operations and dropping munitions on ground forces [6]-[9].

This technology is a serious threat to nuclear security and safety [10]-[12]:

1) The possibility of stealth smuggling of prohibited substances and objects both to and from the protected areas of nuclear facilities and across borders (i.e. nuclear materials, radioactive materials, weapons, ammunition, explosives, RF transmitters that can affect or hack wireless communication etc.);
2) Stealth reconnaissance of the means of nuclear facilities physical protection and the work of security guards from the air or from imperceptible landed drones;
3) Sabotages with possible damage to critical infrastructure elements, blackouts, lots of fires, explosions.

So nuclear facilities not equipped with effective means of detecting and fighting drones are potentially vulnerable to the spread of dangerous materials and terrorist sabotage attacks [13]. But not all existing technologies for detecting and counteracting drones are universal and each of them has advantages and disadvantages [14], [15]. Drones can be very hard to spot and counteract especially if they fly autonomously at high altitudes or in poor visibility conditions.

For example, passive detection systems based on *radio frequency (RF) analysis* are able to detect controlled drones in advance and quickly determine the exact position of its operator. But these systems are weak in detecting autonomous drones or in overcrowded RF environment. *Optical* and *acoustic detection systems* have modest capabilities in range, viewing angle, weather conditions and other parameters. Active systems based on *radar technologies* are universal, but require licenses and measures to prevent harmful interference and potential collateral damage.

Potential collateral damage and restrictions of regulators can also be issues for such effective drone countermeasures as *high power microwave devices* (*HPM*) and *high energy lasers. Jamming radio frequencies* and *spoofing GPS* are useless against drones with autonomous navigation systems and can cause harmful RF interference too. There is also interesting countermeasure where drone-protector catches intruder-drones with nets.

So, most universal and effective anti-drone solutions should combine different detection systems and countermeasures in a way to cover all possible risks. Although it is possible to protect nuclear facilities, the protection of long borders and critical infrastructure from nuclear and radioactive materials smuggling and terrorism by drones is much larger task and huge threat. On the other hand drones can really help in nuclear security by catching or pursuing enemy drones and intruders, or by watching from the air.

Cybersecurity

News about cyberattacks and critical zero-day vulnerabilities found in digital systems appear with alarming frequency [16]-[18]. As practice shows, established approaches in creating software and hardware cannot provide guaranteed invulnerable digital systems. Moreover nuclear facilities can have thousands of different digital systems each of which may have zero-day vulnerabilities. The effects of targeted cyberattacks can be devastating [17]-[19].

Important approaches to ensure cybersecurity should be:

1) Designing important for security digital systems that fundamentally cannot receive data from external networks or standardized data storages such as USB sticks (by using data diodes and unidirectional gateways [20]);

2) Restrictions and access control to safety and security systems;

3) Access control to source codes and documentation of digital systems that are important or can influence on nuclear safety and security;

4) Staff training in cyber-secure ways of working with digital systems;

5) Reasonable limiting or usage control of employee's personal devices. (i.e. software control of prohibited uses or RF analysis of large wireless data uploads);

6) Continuous information monitoring about critical vulnerabilities of systems and quick fixing of them;

7) Restrictions on the use of wireless networks and wireless peripherals devices.

AI Surveillance

As for the new opportunities that technologies provide, I want to mention artificial intelligence (AI) based on Machine Learning. AI really helps in advanced methods to detect drones [21], [22] Also AI tech in combination with video surveillance and bio-identification allows, to recognize people and to analyze their actions with high accuracy. For example, Amazon Go are stores where, surveillance system can monitor all visitors, with the help of cameras and sensors. The system automatically takes into account what visitors took from shelves, what they put back and takes payment for the goods taken from store [23].

So imagine a system that is capable to:

- recognize personnel by face and gait;
- analyze and recognize unusual, suspicious and forbidden behavior for every employer individually;
- detect unknown persons in the protected area or suspicious activities nearby.

Such a system can significantly reduce the risk of unauthorized access to controlled areas and insider threats. It will help to identify threats to nuclear security at an early stage and respond in time.

Conclusions

To ensure nuclear security it is essential, to provide analysis of new threats and new technical and organizational means to counter security threats. This is why such conferences are so important. We can share experiences, ideas and opinions on the threats and threat management techniques, to develop effective up-to-date plans, programs and practices for improving nuclear security. IAEA Member States should include them in the scope of their nuclear security regime to be able to withstand emerging threats of our fast changing world [24].

References

[1] Vijay Kumar "Robots that Fly and Cooperate" *TED 2012*. February 2012 [Online video]. Available: https://www.ted.com/talks/vijay_kumar_robots_that_fly_and_cooperate [Accessed: 1 September 2019]

[2] A. D. Wu, E. N. Johnson, Michael Kaess, F. Dellaert and G. Chowdhary *"*Autonomous flight in gps-denied environments using monocular vision and inertial sensors." Journal Article, *AIAA J. of Aerospace Information Systems (JAIS)*, Vol. 10, No. 4, pp. 172-186, April, 2013

[3] Raffaello D'Andrea, "Astounding Athletic Power of Quadcopters". *TEDGlobal 2013.* June 2013. [Online video]. Available: https://www.ted.com/talks/raffaello_d_andrea_the_astounding_athletic_power_of_quadcopters [Accessed: 1 September 2019]

[4] Raffaello D'Andrea, "Meet the Dazzling Flying Machines of the Future". *TEDGlobal 2016.* February 2016. [Online video]. Available: https://www.ted.com/talks/raffaello_d_andrea_meet_the_dazzling_flying_machines_of_the_future [Accessed: 1 September 2019]

[5] Stephen Dinan, "Drones Become Latest Tool Drug Cartels Use to Smuggle Drugs into U.S.". *The Washington Times. 20 August 2017.* [Online]. Available: https://www.washingtontimes.com/news/2017/aug/20/mexican-drug-cartels-using-drones-to-smuggle-heroi/ [Accessed: 1 September 2019]

[6] Hennigan, W.J. "Islamic State's Deadly Drone Operation is Faltering, but U.S. Commanders See Broader Danger Ahead". *L.A. Times.* 28 September 2017. [Online] Available: http://www.latimes.com/world/la-fg-isis-drones-20170928-story.html [Accessed: 1 September 2019]

[7] "Caracas Drone Attack" in *Wikipedia: the Free Encyclopedia* [Online], 4 August 2018. Available: https://en.wikipedia.org/wiki/Caracas_drone_attack [Accessed: 4 August 2019].

[8] Jonathan Rupprecht "Drone Sabotage on Saudi Pipeline Facility Raises Concerns" *forbes.com* 15 May 2019 [Online]. Available: https://www.forbes.com/sites/jonathanrupprecht/2019/05/15/drone-sabotage-on-saudi-pipeline-facility-raises-concerns/#359c941979dc [Accessed: 1 September 2019]

[9] Adam Morris "ISIS Drone Destroyed SAA Ammo Depot In Deir Ez Zor Stadium". *dailymotion.com* 24 October 2017. [Online video] Available: https://www.dailymotion.com/video/x661t4x [Accessed: 1 September 2019]

[10] Michael Kan "Drones Have Potential for Industrial Sabotage". *IDG News Service.* 4 Aug 2016 [Online]. Available: https://www.computerworld.com/article/3104149/drones-have-potential-for-industrial-sabotage.html [Accessed: 1 September 2019]

[11] The Department of Homeland Security, "Unmanned Aircraft Systems (UAS) - Critical Infrastructure" *The Department of Homeland Security*. March 2019 [Online] Available: https://www.dhs.gov/cisa/uas-critical-infrastructure [Accessed: 1 September 2019]

[12] The Department of Homeland Security, "UAS and Critical Infrastructure – Understanding the Risk" *youtube.com* 3 July 2018. [Online video]. Available: https://www.youtube.com/watch?v=o6x-cj1wXZk [Accessed: 1 September 2019]

[13] Euronews, "Greenpeace Crashed a Drone Into a French Nuclear Power to Highlight Security Issues*." youtube.com* 3 July 2018 [Online video]. Available: https://youtu.be/znolxjFDnKA [Accessed: 1 September 2019]

[14] Robin Radar Systems "9 Counter-Drone Technologies To Detect And Stop Drones Today". *robinradar.com* 22 March 2019 [Online] Available: https://www.robinradar.com/9-counter-drone-technologies-to-detect-and-stop-drones-today [Accessed: 1 September 2019]

[15] I. Güvenç, O. Ozdemir, Y. Yapici, H. Mehrpouyan, and D. Matolak, ''Detection, localization, and tracking of unauthorized UAS and Jammers,'' in Proc. IEEE/AIAA Digital Avionics Syst. Conf. (DASC), Sep. 2017, pp. 1–10. Available: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20170009465.pdf [Accessed: 1 September 2019]

[16] Help Net Security "Vulnerabilities in Siemens' most secure industrial PLCs can lead to industrial havoc". *helpnetsecurity.com*. 9 August 2019. [Online] Available: https://www.helpnetsecurity.com/2019/08/09/siemens-plc-vulnerabilities/ [Accessed: 1 September 2019]

[17] "Cybersecurity - 2018−2019: Results and Forecasts", section: Risky Industry, by Vladimir Nazarov, *ptsecurity.com*, 18 December 2018 [Online] Available: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2018-2019/#id5 [Accessed: 1 September 2019]

[18] Page Stoutland, "Cyberattacks on Nuclear Power Plants: How Worried Should We Be?" *Nuclear Threat Initiative*, 19 March 2018 [Online] Available: https://www.nti.org/analysis/atomic-pulse/cyberattacks-nuclear-power-plants-how-worried-should-we-be/ [Accessed: 1 September 2019]

[19] World Economic Forum "The Global Risks Report 2019 14th Edition" *World Economic Forum*, p.16-17, 2019. [online document]. Available: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf [Accessed: 1 September 2019]

[20] Help Net Security "Detecting PLC Malware in Industrial Control Systems". *helpnetsecurity.com*. 21 February 2019. [Online] Available: https://www.helpnetsecurity.com/2017/02/21/plc-malware-ics/ [Accessed: 1 September 2019]

[21] Unlu, Eren & Zenou, Emmanuel & Riviere, Nicolas & Dupouy, Paul-Edouard. (2019). Deep learning-based strategies for the detection and tracking of drones using several cameras. IPSJ Transactions on Computer Vision and Applications. 11. 10.1186/s41074-019-0059-x. Available: https://www.researchgate.net/publication/334667145_Deep_learning-based_strategies_for_the_detection_and_tracking_of_drones_using_several_cameras [Accessed: 1 September 2019]

[22] Al-Sa'd, Mohammad & Al-Ali, Abdulla & Mohamed, Amr & Khattab, Tamer & Erbad, Aiman. (2019). RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database. Future Generation Computer Systems. 100. 10.1016/j.future.2019.05.007. Available: https://www.researchgate.net/publication/332998480_RF-based_drone_detection_and_identification_using_deep_learning_approaches_An_initiative_towards_a_large_open_source_drone_database [Accessed: 1 September 2019]

[23] "Amazon Go" in *Wikipedia: the Free Encyclopedia* [Online], 4 August 2018. Available: https://en.wikipedia.org/wiki/Amazon_Go [Accessed: 1 September 2019]

[24] International Atomic Energy Agency, "Objective and Essential Elements of a State's Nuclear Security Regime", *IAEA Nuclear Security Series No. 20*, IAEA, Vienna (2013). Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf [Accessed: 1 September 2019]