**Between Scylla and Charybdis:**

**The Threat of Democratized Artificial Intelligence**

Ori Swed[[1]](#footnote-1)

Kerry Chávez[[2]](#footnote-2)

**Abstract**

As artificial intelligence (AI) advances, speculations on its implications run parallel, sometimes rampant. On one side, alarmists foresee a technological singularity as AI outstrips human intelligence. Their focus on locating the event horizon, where tools designed to bring a better future turn against us, precludes the ability to identify tangible, relevant threats. On the other side, scholars and analysts tend to trail behind the staggering speed of development. Called cultural lag, the deliberate pace of theoretical reflection is out of sync with the rapid pace of proliferation, leading to under- and misanalysis. Steering between the Scylla of doomsday scripts and the Charybdis of cultural lag, we identify and discuss the threat of violent nonstate actors (VNSAs) exploiting advanced and democratized AI technologies to commit terrorist attacks. The customary concerns about VNSAs acquiring nuclear, chemical, and biological weaponization capacities have not come to fruition despite how fitting they are for violent agendas. Conversely, seemingly benign technologies such as satellite maps and social media have become quite instrumental in the success of VNSA activity. We posit that what determines VNSA adoption and innovation is the confluence of advanced and democratizedtechnologies. The former feature mitigates the necessity of complex engineering efforts and lowers the technical capacity requisite. The latter introduces the dual-use dilemma, removing barriers to access that regulated technologies inhibit. Using these two elements as predictive crosshairs, we analyze three potential threats becoming available to VNSAs as AI evolves: self-driving cars, internet bots, and 3D printing. Our study contributes a sensible and shrewd approach to threat analysis in the dynamic world of AI development.

Droids with luminous white carapaces stand at attention in droves. A rogue robot shifts its gaze out of turn, foreshadowing the impending uprising. Fast-forward a few scenes and they are pulsing red, crawling like arachnids across their mainframe ‘brain’ to destroy the rest of humanity standing in their way (*I, Robot* 2004). At least this is the mental image many conjure when Artificial Intelligence (AI) is mentioned. Or perhaps one’s personal Platonic form is the Terminator with chinks in his artificial skin exposing the metal understructure and glowing eye (*The Terminator* 1984). Or the alluring Ava with cybernetic chainmail until she disguises it after outsmarting her maker (*Ex Machina* 2014). These analogies are indicative of alarmists who foresee a technological singularity as AI outstrips human intelligence. Their focus on locating the event horizon, where tools designed to bring a better future turn against us, precludes the ability to identify tangible, relevant threats. This is not exclusive to filmography. In popular science, the eminent Elon Musk identifies AI as humanity’s greatest existential threat warning that “we do not have long to act. Once this Pandora’s box is opened, it will be hard to close” (Hern 2017). Scientifically harder still, scholars warn of cyber insecurities arising from AI from the workplace (Huang and Rust 2018, McClure 2018) to hospitals (Pepito and Locsin 2019) to home (Heartfield et al. 2018) and in the traveling infrastructures in between (Ionita 2017). The misconceptions, speculations, and ultimately fear that overestimate doomsday scripts represent a common approach to AI.

The other common response is underestimation of the implications. Called cultural lag, the deliberate pace of social and institutional adaptation is out of sync with the rapid pace of technological innovation. Ogburn (1922) developed the theory of cultural lag to explain periods of maladjustment between parts of modern culture that change at variable rates. Dividing culture into material and non-material elements, he notes that material advancements tend to arrive first as a function of discovery or invention. Aspects of society correlated with the material progress are compelled to adjust in the aftermath. Depending on the nature of the change, the heterogeneity of response, and the inertia of the status quo,[[3]](#footnote-3) periods of maladjustment (or lag) can be protracted and tumultuous. In addition, the compounding rate of change can complicate an otherwise timely transition. Brinkman and Brinkman (1997) observe that “cultures in an advanced stage of economic development…tend to experience an exponential accumulation of material culture given the dynamics of a science-fed technology" (3). The pace and reach of AI’s expansion exemplifies the problem of cultural lag, especially on legal and analytical fronts. Lacking proper understanding of the scope, context, and content of AI applications penetrating several industries, legislation and regulation struggle to keep pace much less anticipate problems. While cultural dissonance might be uncomfortable, the consequences of security oversights are more dire.

Steering between the Scylla of doomsday scripts and the Charybdis of cultural lag, we identify and discuss the threat of violent nonstate actors (VNSAs) exploiting AI to commit terrorist attacks. We posit that what determines VNSA innovation is the confluence of advanced and democratizedtechnologies. The former feature mitigates the necessity of complex engineering efforts and lowers the technical capacity requisite. The latter introduces the dual-use dilemma, removing barriers to access that regulated technologies inhibit. Using these two elements as predictive crosshairs, we analyze three potential threats becoming available to VNSAs as AI evolves: self-driving cars, internet bots, and 3D printing. Our study contributes a sensible and shrewd approach to threat analysis in the dynamic world of AI development.

**Theory – Advanced *and* Democratized**

As a general rule, VNSAs are asymmetrically weak and resource-constrained relative to states. This compels them to adopt unconventional strategies that deflect brute force, attrite the enemy’s political will, and control populations through fear or appeal (Mack 1975, Arreguín-Toft 2001). It also puts a premium on innovation as non-state groups aim to offset asymmetries in capability or effectiveness in any way possible. The criteria for determining how VNSAs decide to adopt an innovation includes desire, capacity, and capability (Horowitz 2010). Capacity refers to technical competence to master and maintain a given platform. Ackerman (2016) traces the determinants of terrorist groups engaging in “complex engineering efforts,” arguing that emerging technologies are making it easier, less costly, and safer. Where before many components, steps, or applications were complex and manually executed, technological progress is producing packages that self-integrate, calibrate, and harmonize. This lowers the technical capacity requisite to adopt increasingly advanced approaches to political violence. AI is a game-changer in this trend. It is infusing not only an unprecedented level of sophistication into myriad subjects, but a stunning pace of development and (self-) learning. In addition to decreasing entry capacity requisites for VNSAs to utilize advanced tech, it will enable ongoing innovation as it optimizes.

While advanced technologies can be expected to enhance a group’s fighting capacity, not all are equally affordable, available, or navigable. Capability, the third criterion for VNSA adoption, refers to the logistical ability to procure the materials, personnel, and knowledge for an innovation. Advanced technologies that remain cost-prohibitive and / or highly regulated are not likely to systematically proliferate to resource-constrained, violent groups. Indeed, despite the considerable attention paid to the danger of terrorists deploying weapons of mass destruction (WMDs), it has not come to fruition. WMDs are both expensive and tightly controlled, constricting VNSAs from enfolding them in their arsenals. We argue that technologies must be democratized, or diffusely and easily available to the average person, in order to be feasibly adopted. First, in order to be operable by the average user, advanced hardware or software must become internally ‘smart’ enough so that despite internal complexity its interface is simple. Second, for technologies that can be used for both benign and malevolent agendas, democratization problematizes regulation. The dual-use dilemma, or the difficulty in curtailing positive and neutral innovations from fear that they will be misused, makes it easier for VNSAs to obtain and retool technologies for their violent agendas (Rath et al. 2014, Rychnovská 2016, Schulzke 2018). Working with ten insurgent groups in the 1980s, Hammes (2019) affirms that they are biased toward democratized tech for reasons of familiarity, confidence, and widespread availability of maintenance.

We assert that it is the confluence of advanced and democratized technologies that most appeal and are amenable to VNSAs. They provide significant augmentation, making them desirable in the context of asymmetry and resource constraints (Wallace and Reeves 2013). Their innate ‘smartness’ lowers the technical capacity requisite to field sophisticated platforms. And they are widely available and affordable, bypassing regulation and cost prohibitions. In the next section, we discuss three confirming cases of VNSA misuse of advanced and democratized tech that validate our theoretical framework—mapping technologies, social media, and civilian drones. We then apply the framework to the field of AI to identify predictive cases. We explore the probabilities that VNSAs will exploit self-driving cars, internet bots, and 3D printing as AI stabilizes in these areas.

**Confirming Cases**

*Google Maps*

Many take for granted the convenience of real-time map guidance at the tap of a button. Originally developed for advanced militaries, modern mapping utilizes Global Positioning System (GPS) infrastructures to pinpoint locations and routing options. Advances in the proliferation and precision of satellite technologies has converted platforms like Google Maps to Google Earth, providing detailed aerial imagery of the entire planet. Importantly, this technology is now open-source and free to anyone with a device with even intermittent internet access. This includes VNSAs. Shortly after Google Maps launched in 2005, violent groups began to exploit the new capabilities. Following raids of insurgent homes in Iraq in 2007, UK troops uncovered evidence that terrorists were using satellite imagery from Google Earth to improve targeting and assaults on allied bases in Basra (Harding 2007). Ribeiro (2008) reports that terrorists used Google Earth to navigate locations in a south Mumbai attack. Al-Qaeda is known to use Google Maps to plan attacks across the entire Middle East (Kredo 2018). In the wake of a plot, which relied heavily on satellite imagery, to explode jet fuel tanks and a pipeline at JFK International Airport, a New York legislator urged Google to blur potential targets. By this point, he was merely “adding to the chorus of critics who say detailed images on Google Earth can aid and abet terrorists and snoops” (Goodin 2011). Google excused itself on the grounds that its data is available on other platforms or can be purchased from commercial entities, highlighting dual-use problems of regulation.[[4]](#footnote-4) Spain’s Centre Against Terrorism and Organised Crime identifies Google Maps as one of three primary vulnerabilities in aviation security, citing that maps enable terrorists to do a significant portion of their planning with accuracy, minimal exposure and opportunity to intercept, and low-cost tools (Flood 2016). Waters (2018) encourages states to tap into open-source maps lacking other reliable intelligence, spotlighting the value of these tools for VNSAs that do not have intelligence apparatuses. Being advanced and openly available, Google Maps have long been and will likely continue to be a regular go-to in the terrorist toolkit.

*Social Media*

Social media is meant to turn distance into digital nearness, reduce costs of interaction, and boost social networks. Largely the domain of college students when it debuted in the early 2000s, it exploded into a pervasive social force. Similar to open-source mapping, all it requires is internet access and a simple computing device for VNSAs to expand their reach and efficacy of influence. Traditionally, violent groups relied on mass media for attention to and distribution of their messages and wider agenda. Social media eliminates this dependency, allowing VNSAs to initiate, craft, and disseminate information at will (Klausen 2015, Melki and Jabado 2016). The breadth and variety of platforms—Facebook, Instagram, Twitter, YouTube, What’sApp, Ask.fm, kik, viper, Tumblr, blogs, dedicated websites, even online gaming portals—enables access to audiences of massively greater size and variety (Conway 2012, Huey 2015, Klausen 2015). Suitable for communication, planning, propaganda, fundraising, and recruiting, social media delivers versatile utility at low cost and easy access (Dean et al. 2012, Awan 2017). At the same time, its decentralized and horizontal structure makes policing difficult (Markon 2016, Melki and Jabado 2016). By virtue of being advanced, user-friendly, and globally democratized, social media has become a primary radicalizing milieu for VNSAs (Huey 2015).

*Civilian Drones*

Industry and intelligence members have been warning of the dangers of commercial-off-the-shelf drones for a long time alongside public reports of their use for narco-terrorism, illicit reconnaissance, and violent attacks. Given their versatility, inexpensiveness, and increasing sophistication driven by commercial competition and demand, they constitute an ideal platform for militant groups (Finisterre and Sen 2016). As early as 2005, analysts began recognizing that drones provide VNSAs with advanced, force-multiplying capabilities (Mandelbaum 2005). Civilian drone technology has only innovated since, becoming increasingly stable and efficient (Friese et al. 2016, Rassler 2016). In line with the theory, these developments lower the technical capacity needed to field drone programs. For example, Libyan fighters in the 2011 march on Tripoli legally procured a user-friendly minidrone from Aeryon Labs. The Vice President of Business Development remarked that “the rebels barely needed a day of training to use a technology that many national armies would love to acquire. We like to joke that it’s designed for people who are not that bright, have fat fingers, and break things” (Ackerman 2011). Notably, it is democratized drones that VNSAs exploit, not high-cost, high-tech, and highly regulated statist models. Civilian models are broadly accessible and affordable. In fact, Ball (2017) notes that their sophistication is increasing at the same rate that costs are decreasing, making drones even more desirable for a resource-constrained actor. The consensus in academic and policy circles is that the nature of the militant drone threat will coincide with commercial advancements (Rassler 2016, Barsade and Horowitz 2017). This confirming case segues well into a discussion of the predictive cases suffused with AI because analysts foresee that drones will attain full autonomy, networked swarming, and emergent intelligence in the near future (Lachow 2017).

**Predictive Cases**

Artificial intelligence, in its simulation and augmentation of human intelligence, radically simplifies the use of advanced technologies. Essentially, it does the complex portions of the work for human operators. Layering AI onto the theory that VNSAs will exploit advanced and democratized technologies only exacerbates the draw, and danger, of the newfound capacities. The three predictive cases share characteristics of the confirming cases, being advanced and currently or predicted to be democratized in a dual-use dilemma format. They differ in their timelines of debut on civilian markets and in the degree to which they can amplify VNSA agendas with the aid of AI.

*Self-driving Cars*

Even a skeptic would likely acknowledge the benefits of autonomous vehicles (AVs): intrinsic adherence to traffic laws, dramatic decreases in accidents (most are caused by human error and judgment), and improved mobility for those unable to drive (Grigorescu et al. 2018, Miller 2018, Rao and Frtunikj 2018). As development drives forward, the prospect of misuse by VNSAs lingers in the back of many minds. In 2015, a research team was able to hack the Lidar system of a self-driving prototype using a simple laser pointer. They warn that cars can be fooled into slowing down or stopping to avoid collisions with phantom obstacles or 'ghost pedestrians.' This follows a 2013 report that other researchers successfully infested AVs with computer viruses causing them to crash by killing the lights and engines and slamming on the brakes (Curtis 2015). Separately, a senior scientist at the RAND Corporation testifies that hacking, especially as an avenue for terrorism, constitutes a significant threat in AVs riddled with cybernetics. She argues that this decreases costs of terrorism as they can commit bombing attacks without sending allegiants to their deaths in suicide attacks (Ravindranath 2017). Australian law enforcement authorities made news by issuing warnings that self-driving cars can be weaponized for terrorism in even simpler ways that preclude hacking and cyber capacities. A rented AV could be packed with explosives, remotely driven to a target site, and detonated from a safe location (Sekhose 2016). Cultural lag comes to the forefront in this technology, as Bradshaw (2018) argues that the danger of weaponization has nothing to do with any particular government, but with the nature of the technology itself. Advancing faster than legislators, regulators, and law enforcement can keep up with, it will be increasingly difficult to police VNSA uses as the technologies mature and go global.

*Internet Bots*

Social bots are automated social media accounts that algorithmically emulate online human activity such that they resist detection (Bessi and Ferrara 2016). They are distinct from internet bots that infect computers with malware for remote control. In computer parlance, we speak of sybils (Ferrara et al. 2016), not zombies (Lee et al. 2008). Their purpose is to drive online traffic and manipulate political communication, opinion and behavior. The direction depends on the algorithm. Thus, the question behind bots is who are the bot masters. Recognizing that organizations ranging from political parties to terrorist groups are running internet bot campaigns, the Defense Advanced Research Projects Agency (DARPA) held a competition for bot detection. Participating teams report that 8.5% of all Twitter users are bots (Subrahmanian et al. 2016). In the 2016 presidential election, Bessi and Ferrara (2016) determine that 1/5 of the entire Twitter conversation about the candidates was generated by bots. Lest critics question whether coding algorithms constitutes too high a capacity for VNSAs, social bots have become sufficiently advanced and democratized for the average person to use. In fact, certain blogs offer ready-made tools and tutorials to customize a bot with no previous coding skills or experience (Bessi and Ferrara 2016). This applies even to current generation bots that convincingly mimic human behavior. They can search the web for information to populate profiles, emulate human circadian rhythms and temporal productive spikes in content generation and consumption, and engage in complex interactions such as entertaining conversations, commenting, and answering questions (Ferrara et al. 2016, Arnaudo 2017, Marr 2018). Given the already profound capacity social media has bestowed on VNSAs, intensifying it with AI agents that outperform human productivity will further advance their goals. Experts worry that this inexpensive, versatile and evolving niche of AI might “shape or reshape communities on a very large scale, in what we might call 'social architecting'" (Hwang et al. 2012, 45). Imagine if VNSAs are the architects.

*3D Printing*

Additive manufacturing, informally called 3D printing, enables the conversion of a three-dimensional computer model into a solid object. Current models are compact, affordable, and rapidly advancing. Theoretically, one could print an infinite number of things to an infinite degree of customization (Blackman 2014). This applies to weapons as easily as to items like life-saving medical modules. The chief fear to date is the prospect of criminals printing guns at will (Little 2014, Walther 2015), but guns are only the beginning of a more imaginative threat analysis. 3D printers can be used to manufacture landmines, improvised exploding devices, small drones, bomblets and munitions, etc. Just as importantly, they can print components for modifications and repairs to maximize a resource-constrained arsenal. AI moves these capabilities forward by leaps and bounds, yielding ‘advanced additive manufacturing.’ First, it increases the speed, scale, and quality of printing by applying deep learning to recognize patterns, detect defections, and improve prefabrication iterations (McCaney 2018, Bharadwaj 2019, Hammes 2019). Second, it is improving design and selection of material properties suitable for a given printing project, serving as an engineering shortcut. LePain (2018) explains that “designers simply enter the desired properties into a program and algorithms predict which chemical building blocks can be combined at a micro level to create a structure with the desired functions and properties." Third, it handles the volume and complexity occurring under the surface of a printing project so that an inexperienced user can generate an accurate and optimized product with little trial and error (Bharadwaj 2019). Finally, emerging applications of AI in 3D printing promise to construct computer models from 2D images, bypassing tedious engineering and coding processes and thereby significantly lowering the technical capacity requisite.

**Conclusion**

The question of how AI might problematize security is new only its manifestation and magnitude. One policymaker remarked that “every major technology—metallurgy, explosives, internal combustion, aviation, electronics, nuclear energy—has been intensively exploited not only for peaceful purposes but also for hostile ones” (Walther 2015). AI is undoubtedly a major technology, and one on the cusp of a cascade into most facets of society. We set out to execute a sensible and shrewd threat analysis at the intersection of AI and international security. On one side, we have endeavored to avoid sensationalist speculations shallowly rooted in context. On the other side, we acknowledge the inertia of cultural lag constraining timely scholarship and policy prescription. To strike a balance, we have asserted a theoretical framework that brackets and concretizes the elements of innovation—desire, capacity, and capability. We have argued that VNSAs are most likely to adopt platforms that are both advanced, being sophisticated enough to lower the technical capacity requisite yet potent, and democratized, being commonplace and affordable for resource-constrained actors. We demonstrated the logic with three confirming cases—mapping technologies, social media, and civilian drones. We then allowed a measure of imagination into the theoretical framework to predict likely VNSA exploitations of AI in the near future. Going forward, we recognize that threat identification is only the first step. Responsible rollouts of AI will need to consider the right governance approach, apportioned between engineers at the front end, legislators and regulators in the middle, and law enforcement professionals at the end. Given the immeasurable potential and utility incubating in AI applications, its advancement is inevitable. What remains is mindful and timely treatments of externalities, unintended consequences, and misuses. May this manuscript be one of them, and may others follow to guide stakeholders in AI’s unfolding.

**References**

Ackerman, G.A. 2016. 'Designing Danger': Complex Engineering by Violent Non-state Actors. *Journal of Strategic Security*, 9(1), pp. 1-11.

Ackerman, S. 2011, Aug 23. Libyan rebels are flying their own minidrone. *Wired*. https://www.wired.com/2011/08/libyan-rebels-are-flying-their-own-mini-drone/.

Arnaudo, D. 2017. Computational Propaganda in Brazil: Social Bots during Elections. *Computational Propaganda Research Project*, Working Paper No. 2017.8.

Arreguín-Toft, I. 2001. How the Weak Win Wars: A Theory of Asymmetric Conflict. *International Security*, 26(1), pp. 93-128.

Awan, I., 2017. Cyber-Extremism: ISIS and the Power of Social Media. *Society*, 54(2), pp. 138-149.

Ball, R.J. 2017. *The Proliferation of Unmanned Aerial Vehicles: Terrorist Use, Capability, and Strategic Implications*. Livermore, CA: Lawrence Livermore National Laboratory.

Barsade, I. and Horowitz, M.C. 2017, Sep 7. Militant groups have drones. Now what? *Bulletin of the Atomic Scientists*. https://thebulletin.org/2017/09/militant-groups-have-drones-now-what/.

Bessi, A. and Ferrara, E. 2016. Social Bots Distort the 2016 U.S. Presidential Election Online Discussion. *First Monday*, 21(11), pp. 1-14.

Bharadwaj, R., 2019, Feb 12. Artificial Intelligence Applications in Additive Manufacturing (3D Printing). *Emerj*. https://emerj.com/ai-sector-overviews/artificial-intelligence-applications-additive-manufacturing-3d-printing/.

Blackman, J. 2014. The 1st Amendment, 2nd Amendment, and 3D Printed Guns. *Tennessee Law Review*, 81, pp. 479-538.

Bradshaw, T. 2018, Jan 14. Self-driving cars raise fears over 'weaponisation'. *Financial Times*. https://www.ft.com/content/a8dbd4e0-f807-11e7-88f7-5465a6ce1a00.

Brinkman, R.L. and Brinkman, J.E. 1997. Cultural Lag: Conception and Theory. *International Journal of Social Economics*, 24(6), pp. 609-627.

Conway, M. 2012. From al-Zarqawi to al-Awlaki: The Emergence of the Internet as a New Form of Violent Radical Milieu. *CTX: Combating Terrorism Exchange*, 2(4), pp. 12-22.

Curtis, S. 2015, Sep 8. Self-driving cars can be hacked using a laser pointer. *The Telegraph*. https://www.telegraph.co.uk/technology/news/11850373/Self-driving-cars-can-be-hacked-using-a-laser-pointer.html.

Dean, G., Bell, P., and Newman, J. 2012. The Dark Side of Social Media: Review of Online Terrorism. *Pakistan Journal of Criminology*, 4(3), pp. 103-122.

*Ex Machina.* 2014. Directed by Alex Garland. Universal City, CA: Universal Studios.

Ferrara, E., Varol, O., Davis, C., Menczer, F., and Flammini A. 2016. The Rise of Social Bots. *Communications of the ACM*, 59(7), pp. 96-104.

Finisterre, K. and Sen, R. 2016, Oct 24. The Unrealized Threat of Weaponized Drones. *Morning Consult*. https://morningconsult.com/opinions/unrealized-threat-weaponized-drones/.

Flood, R. 2016, Sep 27. ISIS using GOOGLE MAPS to plot airport and plane terror attacks, report warns. *The Express*. https://www.express.co.uk/news/world/715011/Isis-airplane-attack-terror-bomb-google-map-report-airport.

Friese, L., Jenzen-Jones, N.R., and Smallwood, M. 2016. Emerging Unmanned Threats: The Use of Commercially Available UAVs by Armed Non-state Actors. *Armament Research Services*. http://armamentresearch.com/wp-content/uploads/2016/02/ARES-Special-Report-No.-2-Emerging-Unmanned-Threats.pdf.

Goodin, D. 2007, Jun 11. Google Maps aids terrorists, NY lawmaker warns. *The Register*. https://www.theregister.co.uk/2007/06/11/google\_maps\_aids\_terrorists/.

Grigorescu, S.M., Glaab, M., and Roßbach A. 2018, Jul 30. From logistics regression to self-driving cars: Chances and challenges for machine learning in highly automated driving. *Embedded Computing*. http://www.embedded-computing.com/automotive/from-logistics-regression-to-self-driving-cars-chances-and-challenges-for-machine-learning-in-highly-automated-driving.

Hammes, T.X. 2019, Feb 25. Technology Converges; Non-state Actors Benefit. *Hoover Institution*. https://www.hoover.org/research/technology-converges-non-state-actors-benefit.

Harding, T. 2007, Jan 13. Terrorists use Google maps to hit UK troops. *Telegraph News*. https://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html.

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J.R.J., Filippoupolitis, A., Roesch, E. 2018. A Taxonomy of Cyber-physical Threats and Impact in the Smart Home. *Computers & Security*, 78, pp. 398-428.

Hern, A. 2017, Sep 4. Elon Musk says AI could lead to third world war. *The Guardian*. https://www.theguardian.com/technology/2017/sep/04/elon-musk-ai-third-world-war-vladimir-putin.

Horowitz, M.C. 2010. Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism. *International Organization*, 64(1), pp. 33-64.

Huang, M.H. and Rust, R.T. 2018. Artificial Intelligence in Service. *Journal of Service Research*, 21(2), pp. 155-172.

Huey, L. 2015. This is Not Your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming. *Journal of Terrorism Research*, 6(2), pp. 1-16.

Hwang, T., Pearce, I., and Nanis, M. 2012. Socialbots: Voices from the Fronts. *Interactions*, 19(2), pp. 38-45.

Ionita, S. 2017. Autonomous Vehicles: From Paradigms to Technology. *IOP Conference Series: Materials Science and Engineering*, 252, pp. 1-8.

*I, Robot.* 2004. Directed by Alex Proyas. Los Angeles, CA: 20th Century Fox.

Klausen, J. 2015. Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38, pp. 1-22.

Kredo, A. 2018, Apr 20. Al Qaeda Using Google Maps to Plan Jihadist Attacks. *Washington Free Beacon*. https://freebeacon.com/national-security/al-qaeda-using-google-maps-plan-jihadist-attacks/.

Lachow, I. 2017. The Upside and Downside of Swarming Drones. *Bulletin of the Atomic Scientists*,73(2), pp. 96-101

Lee, W., Wang, C., and Dagon, D. 2008. *Botnet Detection: Countering the Largest Security Threat.* New York, NY: Springer.

LePain, A. 2018, Dec 11. How AI and 3D Printing are Revolutionizing Materials Design. *R&D Magazine*. https://www.rdmag.com/article/2018/12/how-ai-and-3d-printing-are-revolutionizing-materials-design.

Little, R.K. 2014. Guns Don't Kill People, 3D Printing Does? Why the Technology is a Distraction from Effective Gun Controls. *Hastings Law Journal*, 65, pp. 1505-1513.

Mack, A. 1975. Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict. *World Politics*, 27(2), pp. 175-200.

Mandelbaum, J., Ralston, J., Gutmanis, I., Hull, A., and Martin, C. 2005. Terrorist Use of Improvised or Commercially Available Precision-guided UAVs at Stand-off Ranges: An Approach for Formulating Mitigation Considerations. *Institute for Defense Analyses.* http://www.dtic.mil/dtic/tr/fulltext/u2/a460419.pdf.

Markon, J. 2016, Feb 10. As concern grows over terrorists on social media, Senate bill calls for national strategy. *The Washington Post*. https://www.washingtonpost.com/news/federal-eye/wp/2016/02/10/as-concern-grows-over-terrorists-on-social-media-senate-bill-calls-for-national-strategy/?utm\_term=.43bb08a586cc.

Marr, B. 2018, May 18. How Artificial Intelligence is Making Chatbots Better for Businesses. *Forbes*. https://www.forbes.com/sites/bernardmarr/2018/05/18/how-artificial-intelligence-is-making-chatbots-better-for-businesses/#396362d94e72.

McCaney, K. 2019, Aug 17. AI Fueling Next Wave of 3D Printing and Robotics. *Government CIO*. https://governmentciomedia.com/ai-3d-printing-robotics.

McClure, P.K. 2018. "You're Fired," Says the Robot: The Rise of Automation in the Workplace, Technophobes, and Fears of Unemployment." *Social Science Computer Review*, 36(2), pp. 139-156.

Melki, J. and Jabado, M. 2016. Mediated Public Diplomacy of the Islamic State in Iraq and Syria: The Synergistic Use of Terrorism, Social Media and Branding. *Media and Communication*, 4(2), pp. 92-103.

Miller, M. 2018, Dec 11. Consumer groups say Senate's revamped self-driving car bill fails to resolve cyber, safety concerns. *Inside Cyber Security*. https://insidecybersecurity.com/daily-news/consumer-groups-say-senates-revamped-self-driving-car-bill-fails-resolve-cyber-safety.

Ogburn, W.F. 1922. *Social Change with Respect to Culture and Original Nature.* New York, NY: B. W. Huebsch, Inc.

Pepito, J.A. and Locsin, R. 2019. Can Nurses Remain Relevant in a Technologically Advanced Future? *International Journal of Nursing Sciences*, 6, pp. 106-110.

Rao, Q. and Frtunikj, J. 2018. Deep Learning for Self-driving Cars: Chances and Challenges. *ACM / IEEE Workshop on Software Engineering for AI in Autonomous Systems*.

Rassler, D. 2016. Remotely Piloted Innovation: Terrorism, Drones, and Supportive Technology. *USMA Combating Terrorism Center.* http://www.dtic.mil/dtic/tr/fulltext/u2/1019773.pdf.

Rath, J., Ischi, M., and Perkins, D. 2014. Evolution of Different Dual-use Concepts in International and National Law and Its Implications on Research Ethics and Governance. *Science & Engineering Ethics*, 20, pp. 769-790.

Ravindranath, M. 2017, Feb 15. Lawmakers Want Self-driving Cars to Thrive But Still Fear Hacks. *NextGov*. https://www.nextgov.com/emerging-tech/2017/02/lawmakers-want-self-driving-cars-thrive-still-fear-cyber-hacks/135437/.

Ribeiro, J. 2008, Nov 30. Google Earth Used by Terrorists in India Attacks. *PC World*. https://www.pcworld.com/article/154684/article.html.

Rychnovská, D. 2016. Governing Dual-use Knowledge: From the Politics of Responsible Science to the Ethicalization of Security. *Security Dialogue*, 47(4), pp. 310-328.

Schulzke, M. 2018. Drone Proliferation and the Challenge of Regulating Dual-Use Technologies. *International Studies Review*, 0, pp. 1-21.

Sekhose, M. 2016, Nov 8. Australian authorities fear self-driving cars could be used for terrorism. *BGR Media*. https://www.bgr.in/news/australian-authorities-fear-self-driving-cars-could-be-used-for-terrorism/.

Subrahmanian, V.S., Azaria, A., Durst, S., Kagan, V., Galstyan, A., Lerman, K., Zhu, L., Ferrara, E., Flammini, A., and Menczer, F. 2016. The DARPA Twitter Bot Challenge. *Computer*, 49(6), pp. 38-46.

*The Terminator.* 1984. Directed by James Cameron. Los Angeles, CA: Hemdale Film Corporation.

Wallace, D. and Reeves, S. 2013. Non-state Armed Groups and Technology: The Humanitarian Tragedy at our Doorstep? *University of Miami National Security & Armed Conflict Law Review*, 3(1), pp 26-45.

Walther, G. 2015. Printing Insecurity? The Security Implications of 3D-Printing of Weapons. *Science & Engineering Ethics*, 21, pp. 1435-1445.

Waters, N. 2018, Sep 25. Google Maps is a Better Spy than James Bond. *Foreign Policy*. https://foreignpolicy.com/2018/09/25/google-maps-is-a-better-spy-than-james-bond/.

1. Texas Tech University, Department of Sociology, ori.swed@ttu.edu [↑](#footnote-ref-1)
2. Texas Tech University, Department of Political Science, kerry.chavez@ttu.edu [↑](#footnote-ref-2)
3. Cultural inertia can derive from social habits, binding powers of tradition, vested interests, bureaucratic obstinance, and even fear-based conformity to the past (Brinkman and Brinkman 1997). [↑](#footnote-ref-3)
4. For instance, Planet sells sub-meter resolution images online, taken by cube satellites of the entire globe every day. SpyMeSat is a mobile app that offers on-demand access to hi-resolution satellite imagery (Hammes 2019). [↑](#footnote-ref-4)