AI, Urban Warfare and Cyber Warfare: Ethical and Anticipated Ethical Issues

Richard L Wilson[1], and Noah Donnelly[2]
[1]Department of Philosophy/Computer Science and Information Sciences, Towson University, Baltimore, Maryland, USA
[2]Computer Science and Information Sciences, Towson University, Baltimore, Maryland, USA

wilson@towson.edu
ndonnel1@students.towson.edu

Abstract: The integration of AI into urban warfare and cyber warfare is reshaping the landscape of military operations. AI i s being leveraged to enhance military capabilities, improve defense strategies, and address the evolving threat environmen t in military operations. AI has had an influence in these fields in the following areas: (1) in Urban warfare AI technologies are being integrated into smart city projects reshaping urban environments and operational strategies directed at smart cities. (2) In Cyber warfare AI is transforming cyber warfare by enabling faster destructive digital attacks. It is being employed to develop new categories of cyber weapons including autonomous malware and deepfake-driven disinformation and misinformation campaigns. (3) In military operations AI is reshaping military operations by improving speed, scale and clandestine attacks as well as enhancing mission command and network resilience. (4) In Cyber defense AI is being utilized to leverage AI proactive threat identification, automated incident response and predictive analytics are used to counter AI-driven threats. This analysis will focus on ethical and anticipated ethical issues with AI, Urban Warfare and Cyber Warfare to AI autonomous cyber warfare. The method that is employed is a standard conceptual analysis of key issues, combined with careful definitions of terminology including key applications of conceptual distinctions applied to case studies. The method of ethical analysis follows the standard practice of applying ethical concepts and terms issues within case studies. The issues that will be addressed will include (1) The idea of machines making independent decisions about targeting and attack execution without human "in the loop" oversight is deeply troubling. (2) Accountability: If an autonomous AI system causes widespread damage or civilian harm, who is responsible? The programmer? The commander who authorized its deployment? The AI itself? (3) Escalation Control: How can the use of autonomous cyber weapons be controlled to prevent unintended escalation of conflict? A rapid, AI-driven counterattack might be perceived as a disproportionate response, triggering a spiral of retaliatory actions. (4) Unintended Consequences: AI systems, while powerful, can be unpredictable. A bug or an unforeseen interaction could lead to catastrophic outcomes that were never intended by human operators. These concerns highlight the urgent need for international dialogue and the establishment of norms around the development and use of AI in warfare.

Keywords: Smart cities, Autonomous malware, Human-in-the-loop, The gospel (AI), DeepLocker, Flash war, Anticipatory ethics, Sociotechnical imperative, Algorithmic accountability

1. Introduction

A feral city is a city in which the government has lost the ability to maintain the rule of law but remains a functioning actor in the greater international system (Kilcullen, 2012). In such a situation Kilcullen further writes that these cities are not destroyed, they are controlled by gangs, warlords, and insurgents. Urban environments are becoming the primary battlefield in which warfare takes place in the 21st century. We are currently witnessing the combining of Urban and Cyber Warfare through the Internet of Military Things (IoMT).

Urban warfare can be defined as an armed conflict that is fought within densely populated areas, built up areas like towns and cities. Urban warfare is characterized by close quarters combat within and complicated by three-dimensional environments. It is considered the most deadly and challenging form of combat (EBSCO, 2025). Key aspects of urban warfare include: "The Urban Triad", 360-degree threats, heightened tactical challenges, civilian and humanitarian crises, and massive defensive advantages. The Urban Triad is defined by the United States Department of Defense as consisting of "A complex manmade physical terrain", "A population of significant size and density", and "An infrastructure upon which the area depends" (United States. Joint Chiefs of Staff, 2002). The 360-degree threats come from enemies occupying buildings, who can fire upon columns from all angles. Heightened tactical challenges come from unclear lines of sight, dense building areas causing air support to be limited, and making it harder to target enemy positions without injuring and killing non-combatants. Civilian and Humanitarian crises are caused by warfare being conducted in densely populated urban areas, with civilians and non-combatants being caught in the crossfire, although **urban warfare is not limited to just this** (ICRC, n.d.). The defensive advantages of urban warfare stem from attackers in streets and fields outside the city having very little cover, compared to those in the city having ample cover and opportunities to reposition.

A Smart City is an urban area that uses Internet of Things (IoT) sensors to operate which involves gathering data, and managing assets, including but not limited to traffic, power, and first responders (IBM, n.d.). All of this is coordinated to provide real-time data to optimize city services like traffic flow and energy consumption. Smart cities also aim at improving public transit and having faster emergency responses. This is a utopian view, to accomplish any of this one must have access to all the **data in the smart city**, intimate daily routines, and be willing to be subject **everyone** to mass surveillance. Key technologies in smart cities include IoT sensors for monitoring, Artificial Intelligence to make sense of all the collected data, and high speed, secure networks for the transmission of massive amounts of data (Chini, 2025).

To understand the remainder of this **analysis**, Autonomous Cyber Weapons must also be understood. These are special types of cyber weapons where Malware uses AI to change its behavior, to avoid detection and select targets autonomously. This was demonstrated with DeepLocker's presentation by Stoecklin in 2018. DeepLocker **like software** is the future of cyber warfare, a danger which current threat detection systems, cannot address. This paper argues that integrating AI into cyber and urban warfare creates what can be called a hyper war environment. A hyper war environment **can potentially** outpace human cognition and violates the principle of meaningful human control over systems while creating systemic risks of accidental escalation.

2. Technical Issues

To understand current ethical issues as well as future technical and ethical issues related to the use of AI in urban and cyber warfare, we must understand the current landscape of cyber and urban warfare in smart cities.

2.1 Smart Cities as Attack Surfaces

Smart cities rely on their digital twin, which is a dynamic, virtual replica and duplicate of the physical urban infrastructure (Halúsková, 2023). The fact that the technical infrastructure of smart cities relies upon digital twins makes them uniquely vulnerable to attack. Digital twins combine IoT sensors, 3D modeling, and Artificial Intelligence (AI) to monitor, simulate and optimize city operations in real time (Weil, 2023). The digital twin opens a new attack surface, if an attacker can hack the digital twin, they effectively gain control over the city. **Once** a theoretical hacker has control of the digital twin, they can conceivably alter sensor readings to create false states, which forces systems to run outside safe limits causing **cascading** disruptions including blackouts or water shortages. If attackers wanted **to escalate** beyond simulated digital attacks and plan a kinetic attack, the digital twin serves as a model for constructing a blueprint for infrastructure targeting attacks. If a hacker wanted to cause chaos **within an urban environment** they could tamper with traffic management, e.g., turning every light green, or to halt operations turning every light red. If attackers wanted money, they could hold the cities management system hostage (Abreu et al., 2021).

2.2 Weaponizing Infrastructure

While smart cities are going to provide a prominent attack surface for cyber war, they are not the only vulnerable targets. Even if a city is not a "smart city" per se, **such a city can still** have vulnerabilities similar to smart cities, **they are** just attacked by different means. While traditional cyber-attacks can be effective against **smart** cities, AI can be weaponized as a means to make these attacks faster, more precise, and automated. Adversaries can leverage AI's capabilities for reconnaissance, developing adaptive malware, conducting highly sophisticated social engineering **operations**, and coordinated physical disruptions upon cities (New Jersey Cybersecurity and Communications Integration Cell [NJCCIC], n.d.). This **can result in** what is called Hybrid Warfare. Hybrid Warfare is a combination of digital and kinetic attacks to maximize the effectiveness of an assault. AI can be used to manipulate ordinary activities in an urban environment as well as military activities by manipulating traffic lights to block a military convoy, shut off the power grids disabling hospitals, or identify specific soldiers or vehicles for targeting (NATO, 2025).

2.3 AI in Mission Command

Urban environments are incredibly dense; **which** creates a phenomenon where troops are operating in what is effectively a series of canyons. **Cities are** a series of canyons in the sense that skyscrapers block satellite signals (GPS) and line-of-sight communications. The *Joint Publication 3-06: Doctrine for Joint Urban Operations* states urban terrain is characterized by a multi-dimensional battlespace that involves three layers: subsurface (sewers), surface (streets), and the supersurface (skyscrapers and other tall buildings) (United States, Joint Chiefs of Staff, 2002). This creates **a complex and potentially** chaotic environment where humans can be too slow to issue temporally effective commands, thus creating the need for the introduction of AI into mission command **and control.** AI algorithms are increasingly used to fuse together data from various sensors (drones, CCTV, soldier wearables) to create a coherent "Common Operating Picture" (COP) when traditional communications are disabled. AI provides a unique advantage, but also a unique risk. The “fog of war” that is found in dense cities can often cause commanders to be overwhelmed from an overload of information. **While AI systems can process a massive amount of data, these systems can also be overloaded and become potentially** overwhelmed. They can process thousands of feeds simultaneously and can identify incoming threats employing these automated systems **but even they can be overwhelmed**. Reliance on AI for navigation and threat detection is dangerous because AI relies on its pre-trained data. If AI encounters a new threat with data that it has not previously seen, like a specific type of barricade, **AI could lead soldiers into a trap because the AI thought that the barricade was part of a safe path forward.**

2.4 Autonomous Malware

Traditional malware relies on conditionals in programming such as **“if-then”** statements. With hypothetical statements a task is executed if and once a **specific** criterion is met. AI driven malware **can supplant** these traditional conditionals. A recent impressive example of AI driven malware is DeepLocker, a proof of concept developed by IBM (Stoecklin, 2018). It looks for specific “keys” to unlock the **target**. Those keys could be anything from geolocation data to a person’s face or voice. This means that instead of traditional monitoring for activity, **Deeplocker identifies and attacks the intended target using their biometrics**. Until AI confirms the target’s identity with a high degree of confidence, the malware acts as the benign app which actually hides the malware inside the software. Traditional malware is detectable because these triggers will decrypt the payload, but those triggers are predictable. This is because the malicious code would only decrypt itself in the presence of the malwares desired victim (Kirat et al., 2018), which makes detection much more difficult. This allows cyber-attackers to operate similar to snipers instead of **employing** machine guns. Attackers no longer need to infect and brick thousands of devices to hit their target, they can infect millions of devices and detonate one.

3. Ethical Issues

The integration of similar to DeepLocker and other malicious malware into urban and cyber operations within urban warfare introduces systemic technical and ethical failures that challenge the core tenets of Just War Theory, basic ethical principles and International Humanitarian Law. **The focus of ethical analysis involves a series of factors that expand upon the notion of the performance of an action. As Furrow states, ethics is related to evaluating actions, and actions are performed by those capable of being moral agents. As Furrow says, “When we evaluate an action, we can focus on various dimensions of the action. We can evaluate the person who is acting, the intention or motive of the person acting, the nature of the act itself, or the consequences.” (Furrow, 2005) When malware interventions occur related to AI in Urban warfare and adversaries act, and these actions are based on intentions, these intentions and actions are aimed at producing outcomes. Identifying threats to Urban environments in urban warfare, has never been more evident. The fate of those at risk in urban warfare through urban warfare and cyber warfare are currently critical issues.**

3.1 Accountability Gap

The introduction of AI into urban and cyber warfare introduces an important ethical dilemma known as the accountability gap. If an autonomous AI recommends a strike on a school or hospital because it incorrectly identified a shape as a weapon, who is the responsible party for this crime against civilians? The global legal system relies on the concept of mens rea, which is the guilty mind. Algorithms do not harbor ill will, they do not harbor any will, meaning they cannot meet the criteria of mens rea. The programmer of the AI is far too removed from the process of a strike to ever be held accountable for a bug in its code, they are not an active participant in the conflict. The military commander may have relied on the AI’s processing **power to decide** and may argue that they acted on the best intelligence available to them. Nobody in this chain from the creation of AI to the decision to eliminate a target meets the criteria for having a guilty conscious. This leads to a legal vacuum where war crimes just become “glitches,” and leave victims with no way to **have access to** justice (Human Rights Watch, 2016).

3.2 Escalation Control

When AI enters into conflict with the AI of adversaries, as when AI malware attacks an AI firewall, the interaction happens at speeds in the nanoseconds, which far exceed any conceivable human reaction times. This introduces the possibility of a “Flash War.” Just as “Flash Crashes” (Investopedia, 2024) occur in high frequency trading where a stock market crash occurred in a matter of moments, flash wars can escalate from a skirmish between the AI systems of two adversarial nations, into a full-scale kinetic conflict before humans could intervene.

Automated defense systems might misinterpret a digital probe for information as an imminent nuclear launch and then launch its own preemptive retaliatory strike. This activity would completely bypass human checks that are designed to prevent accidental wars and deaths (Allen & Chan, 2017).

3.3 Meaningful Human Control vs. OODA Loop

"Meaningful Human Control" would require that a human operator have the time and contextual awareness to intervene in a lethal decision before the decision is made to attack an adversary (Santoni de Sio & van den Hoven, 2018). In hyper-war, the OODA (Observe-Orient-Decide-Act) loop once AI is introduced is too fast for humans to keep pace with **AI.** If the human operator cannot understand why the AI has selected a target in the three seconds preceding the opportunity to reverse the decision has closed, the human can have little control over the decision. The consequence is that **in** hyper-war, human input can be irrelevant, by the time the operator can react immense damage has already been caused to the target. This also serves the purpose of degrading the moral agency that operators have over the actions of the systems they maintain, operators of AI systems are merely rubber stamping decisions made by AI (Ekelhof, 2019).

3.4 Principle of Distinction in Smart Cities

Integrating military AI into cyber warfare conducted within smart cities fundamentally violates the principle of distinction in just war theory, which means that civilian and military targets must remain transparently separate. Within smart cities this situation becomes even more complex. When a military uses the same organizational infrastructure in the smart cities that it relies upon for military operations, whether it is the 5G towers, traffic cameras, and civilian power grids, this identifies the entire city as a potentially valid military target. Cyberattacks that intend to disable the military will harm systems meant to sustain civilian life (hospitals, water treatment), which leads to unnecessary **civilian** collateral damage (NATO, 2015).

4. Case Studies

The following four case studies illustrate the real-world application and ethical complexity introduced by the technologies into the issues of the introduction of AI into urban and cyber warfare of these technologies.

4.1 The Gospel (2023-2024)

The recent conflict in Gaza has produced several ethical controversies, one important issue being the use in cyber warfare of the AI system known as "The Gospel" employed by the IDF. The system works by gathering an array of drone footage, intercepted communications, and topographical data to generate recommendations for airstrikes. It identified targets at a rate of 100 per day, as opposed to the dated methods that generated 50 per year, often human selected (Davies, 2023). As stated earlier in the paper, human cognition cannot has a difficult time keeping up with the speed of the AI. This is an example of where humans become a rubber stamp on the machine's decision, because at times operators approved targets being struck in as little as 20 seconds (Schmitt, 2024). While a human can attempt to verify a target in 20 seconds, there is a high error rate under such time constraints. The human trying to keep up with the speed of AI becomes a liability shield rather than a moral agent (Abraham, 2023).

4.2 Ukraine (2022-Present)

In the Russo-Ukraine war many innovations in warfare have been made, one of them is a new spin on an old trick: civilian intelligence networks. Using software from Palantir and other tech firms, Ukraine gathers reports from civilians using chatbots and combines this data with satellite imagery to track Russian soldiers and mark targets for drone operations or artillery strikes (Bienvenue et al,. 2025). While tactically efficient, this comes with a variety of ethical issues, one of which is the blurring of the Principle of Distinction. If a civilian uses their phone to feed targeting data to a military AI, have they now become a combatant? A civilian is effectively acting as a scout for the military, which throughout the history of warfare makes them acceptable targets for militaries. This blurring effectively makes every civilian device a potential military node and those using these devices military targets (Ignatius, 2022).

4.3 Stuxnet (2010)

While Stuxnet is not considered AI, Stuxnet was somewhat autonomous, it was a precursor and serves as the historical warning for autonomous cyber weapons. Thes pseudo autonomous nature of Stuxnet came from it being designed to search for a specific software within the Iranian nuclear plants and execute its program without any human user explicitly instructing it to do so. It only executed after running a complex verification process to ensure it was in the correct facility. First, it looked for Siemens S7-300 and S7-417 programmable logic controllers. It then checked to see if the PLCs were connected to the frequency converter drives it was looking for operating at very high frequencies. Finally, it looked for arrays of 984 devices (matching the centrifuge cascades at Natanz), and if those conditions were not met, it would not activate, which shows a semi-intelligent nature. Although its design involved autonomous behavior and it was precisely targeted, it eventually escaped Natanz and infected over 200,000 computers globally. This illustrates the problem with autonomous weapons, once they are released, the creator loses control over their proliferation (Zetter, 2014).

4.4 Digital Twin Vulnerabilities

While not a specific case, it is important to mention studies on vulnerabilities of the digital twins in smart cities. As cities have been integrating IoT sensors for varying purposes (Chini, 2025), they created a “Digital Twin,” which is a virtual clone of the city that is used for the operation and management of smart cities. It has been demonstrated by researchers, specifically Weil et al. (2023) that Digital Twins are often unsecured. Unlike traditional sieges of fortifications such as cities, you don’t need an army to attack a digital twin, it could be done from a laptop in Moscow. The attack could start by targeting the digital twin and then move from this attack to an attack on an actual city. When the unsecured digital twin is attacked, services like water treatment, traffic lights, and data for first responders can be attacked and crippled. A study by the Center for Long-Term Cybersecurity (CLTC) found that smart city technologies usually lack basic encryption, making them easy entry points for adversaries to pivot into critical networks (Abreu et al., 2021). An example of how a smart city could be attacked would be, if a state actor were able to trick the “Smart Transport” system into a deadlock. While the state physically attacks a city, it could prevent civilians and forces from fleeing, turning efficiency algorithms into death traps.

5. Anticipatory Ethics

Anticipatory Ethics is an ethical framework which focuses on the anticipation and identification of potential ethical issues relating to new and emerging technologies before the technologies become fully developed and entrenched (Brey, 2012). Anticipatory ethics is focused on developing technologies and ethical issues that may emerge as these technologies continue to develop. Applying the "Moral Responsibility for Computing Artifacts" framework (Miller et al., 2011) allows us to foresee and map the ethical obligations of the developers building AI to be employed in urban warfare and cyber warfare.

5.1 Foreseeability of Effect

There are 2 rules that apply from the rules for computing artifacts to the use of AI in cyberwarfare. First, rule 1 states that "The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact." It is foreseeable that autonomous cyber weapons such as DeepLocker and more modern developments once they are released into a smart city will be reverse engineered by state and non-state actors once the original technology has been deployed. Unlike physical missiles, cyber weapons can break out of confinement and wreak havoc on unsuspecting and uninvolved populations. Developers have a moral duty to build either expiration dates or kill switches into their weapons to prevent them from spreading indefinitely. An example of this being done was the kill switch built into the WannaCry malware, where if a specific website domain was registered, then the malware would become benign, and with 10 dollars and 69 cents, the malware was disabled (Cloudflare, n.d.). Releasing an autonomous weapon without a recall mechanism is a direct violation of Rule 1.

5.2 Sociotechnical Imperative

Second, rule 4 states that the "People who design... can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded." Smart cities are designed for sterile, peaceful environments to optimize efficiency for civilian life. This intention does not violate the Sociotechnical Imperative until the fact becomes known that they have been militarized by integrating dual-use surveillance censors. This is embedding civilian technology into a military environment as well as military technology into a civilian environment, which violates the social contract between the government and the city’s residents. Designers need to anticipate these misuses and harden these technologies against military commandeering. Failing to separate and segregate civilian data from military targeting algorithms endangers the entire urban population (Brey, 2012).

6. Recommendations

To mitigate the risks of "Hyper-War" within smart city's and urban cyber-sieges, we propose the following three technical guardrails.

6.1 Digital Airgaps for Critical Urban Infrastructure

To protect smart cities from being weaponized, services and systems that are critical for supporting urban necessities like water, hospital power, and sewage must be physically and logically air gapped from the internet and only support local connections. Cities should implement "Data Diodes" (Owl Cyber Defense, 2025). These are hardware devices that allow date to flow in only one direction, in this case the direction would be flowing out for monitoring. This ensures that no incoming command can reach the control systems from the outside internet. This would effectively prevent an adversary from hacking the digital twin to shut down life supporting systems (NATO, 2025). This recommendation is not without ethical justification. A digital air gap would restore the Principle of Distinction for AI and cyber warfare operations. If the physical civilian life support layer can be separated from the information layer, this can help ensure that cyber war cannot target smart city infrastructure which if successfully targeted and disabled could lead to a public health crisis.

6.2 Algorithmic Circuit Breakers

Algorithmic Circuit breakers must be hard coded into military AI systems to prevent accidental escalations caused by skirmishes between two military AI systems. The technical implementation would look like autonomous software modules that monitor "heat" levels, which would operate depending on how severe the skirmishes between opposing AIs become. The idea of AI moderating AI presents a variety of issues, but since the speed of military AI systems outpace human cognition, there is no other plausible way. If the system escalates conflict above a pre-defined threshold, such as 50 cyber-attacks per second, the circuit breaker would automatically trip and pause all offensive operations pending human review. For autonomous cyber weapons to be used ethically, there must be some sort of meaningful and legitimate human control, which this recommendation restores. It ensures that no machine-speed escalation can spiral into total war without a human explicitly deciding to continue the fight (Allen & Chan, 2017).

6.3 Cryptographic Provenance

To counter data poisoning, all military and civilian sensors must implement cryptographic signing. Every video frame from a drone or command rom HQ must be digitally signed with a private key at the point of collection, for a video recording it would be the camera sensor. The receiver then verifies the public key, and any data that lacks the signature is automatically marked as untrustworthy. This preserves Epistemic Integrity. This maintains a verifiable "Chain of Custody" for all information flowing through smart sensors, it can even be applied to commands given by verifiable operators to machines. This secure chain of custody for information is essential to prevent AI from being tricked by adversaries into attacking false targets within smart city infrastructures (Chesney & Citron, 2019).

7. Future Work

Future analysis must expand and move byondbeyond current AI capabilities to the domain of "Agentic AI" where autonomous agents would be capable of negotiating, planning, and executing multi-stage cyber operations without human intervention. As the speed of conflict surpasses human cognitive limitations, the pressure to delegate lethal authority to algorithms will increase. Future research should investigate the "Moral Math" of these algorithms: can an AI be coded to understand the Law of Armed Conflict (LOAC) better than a human soldier, or does the removal of human empathy from the kill chain inevitably lead to the possibility of atrocities? (Scharre, 2018). In addition, the rise of Cognitive Warfare in the Metaverse requires urgent study into how immersive psychological operations (PSYOPS) will impact the operations related to urban and cyber warfare within the domain of civilian mental health.

8. Conclusion

The convergence of AI, Urban Warfare, and Cyber Warfare is creating a "Hyper-War" environment that fundamentally challenges the laws of armed conflict. The ability of AI to turn a smart city's infrastructure into a weapon, or to conduct "sniper" malware attacks via more modern platforms than DeepLocker, represents a shift from *attrition* warfare to *algorithmic* warfare. While these technologies offer tactical advantages in terms of speed and efficiency, they introduce catastrophic strategic risks: the possibilities include the erosion of accountability, the lowering of the threshold for conflict, and the danger of accidental escalation. We need to stop viewing AI as merely a "tool" in the military's kit and recognize it as a potentially independent agent that requires strict, globally enforced ethical constraints. Without these guardrails, specifically digital airgaps, circuit breakers, and provenance verification, the efficiency of the "Smart City" can become weaponized and the smart city infrastructure can be turned against the inhabitants of the smart city while turning a smart city into a lethal "Feral City."

Ethics Declaration: No human participants or personally identifiable information were involved. All data sources were publicly available.

AI Tools Declaration: ChatGPT 5.1 for drafting and refinement. Human authors verified all content. Gemini 3.0 pro used for aiding in sourcing.

References

Abreu, G. M., Pan, A., Post, A. E., Malkin, N., & Frick, K. T. (2021). *How do cyber-risks vary across smart city technologies?* Center for Long-Term Cybersecurity. https://cltc.berkeley.edu/wp-content/uploads/2021/03/Smart_City_Cybersecurity.pdf

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs.

Arkin, R. C. (2009). *Governing lethal behavior in autonomous robots*. Chapman and Hall/CRC.

Bienvenue, E., Kelton, M., Rogers, Z., Sullivan, M., & Ford, M. (2025, December 1). *Private tech companies, the state, and the new character of war*. Carnegie Endowment for International Peace. https://carnegieendowment.org/russia-eurasia/research/2025/12/ukraine-war-tech-companies

Brey, P. A. E. (2012). Anticipatory ethics for emerging technologies. *NanoEthics*, 6(1), 1–13.

Chesney, B., & Citron, D. (2019). Deepfakes and the new disinformation war. *Foreign Affairs*, 98(1), 147–155.

Chini, M. (2025, October 3). *How smart cities are transforming modern construction*. Giatec Scientific. https://www.giatecscientific.com/education/how-smart-cities-are-transforming-modern-construction/

Cloudflare. (n.d.). *What was the WannaCry ransomware attack?* https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

Davies, H. (2023, December 1). 'The Gospel': how Israel uses AI to select bombing targets in Gaza. *The Guardian*. https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets-in-gaza

EBSCO Information Services. (2025). *Urban warfare*. Research Starters: Military History and Science. https://www.ebsco.com/research-starters/military-history-and-science/urban-warfare

Ekelhof, M. A. C. (2019). Moving beyond semantics on autonomous weapons: Meaningful human control in operation. *Global Policy*, 10(3), 343–348.

Furrow, Dwight. Ethics Key concepts in Philosophy, Continuum Press, 2005.

Greenberg, A. (2022, March 31). Russia's cyberwar on Ukraine is a blueprint for what's to come. *Wired*. https://www.wired.com/story/russia-cyberwar-ukraine-blueprint-what-to-come/

Halúsková, B. (2023, May 29–31). *Digital twin in smart city* [Paper presentation]. TRANSCOM 2023: 15th International Scientific Conference on Sustainable, Modern and Safe Transport, Zilina, Slovak Republic.

Human Rights Watch. (2016). *Killer robots and the concept of meaningful human control*. https://www.hrw.org/news/2016/04/11/killer-robots-and-concept-meaningful-human-control

IBM. (n.d.). *What is a smart city?* IBM Think. https://www.ibm.com/topics/smart-city

Ignatius, D. (2022, December 19). How the algorithm tipped the balance in Ukraine. *The Washington Post*.

International Committee of the Red Cross. (n.d.). *Urban warfare and violence*. https://www.icrc.org/en/law-and-policy/urban-warfare-and-violence

Investopedia. (2024, January 3). *Flash Crash: Definition, Example, and Causes*. https://www.investopedia.com/terms/f/flash-crash.asp

Kilcullen, D. (2013). *Out of the mountains: The coming age of the urban guerrilla*. Oxford University Press.

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, 79(1), 1–14.

Kirat, D., Jang, J., & Stoecklin, M. (2018, August 8). *DeepLocker: Concealing targeted attacks with AI locksmithing*. Black Hat USA 2018, Las Vegas, NV, United States. https://research.ibm.com/publications/deeplocker-concealing-targeted-attacks-with-ai-locksmithing

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, 10(4), 415–453.

Miller, K. W., Wolf, M. J., & Grodzinsky, F. S. (2011). Moral responsibility for computing artifacts: 'The Rules'. *IT Professional*, 13(3), 57–59.

NATO Supreme Allied Commander Transformation. (2015). *Urbanization project*. NATO.

New Jersey Cybersecurity and Communications Integration Cell. (n.d.). *AI, APT campaigns, and urgent threats to critical infrastructure*. https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/ai-apt-campaigns-and-urgent-threats-to-critical-infrastructure

Owl Cyber Defense. (2025, July 8). *What is data diode technology & how does it work?* https://owlcyberdefense.com/blog/what-is-data-diode-technology-how-does-it-work/

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Payne, K. (2018). Artificial intelligence: A revolution in strategic affairs? *Survival*, 60(5), 7–32.

Roff, H. M. (2014). The strategic robot: A playbook for computer network attack, defense, and deterrence. *Ethics and Information Technology*, 16(3), 213–227.

Santoni de Sio, F., & van den Hoven, J. (2018). Meaningful Human Control over Autonomous Systems: A Philosophical Account. *Frontiers in Robotics and AI*, 5, 15. https://doi.org/10.3389/frobt.2018.00015

Schmitt, M. N. (2024, June 28). *Israel – Hamas 2024 symposium – The Gospel, Lavender, and the law of armed conflict*. Lieber Institute West Point. https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.

Singer, P. W. (2009). *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin.

Taddeo, M. (2017). The limits of deterrence in cyber conflict. *Philosophy & Technology*, 30(3), 339–355.

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*, 558(7709), 296–298.

UN-Habitat. (2020). *World cities report 2020: The value of sustainable urbanization*. United Nations.

United Nations Department of Economic and Social Affairs. (2018). *68% of the world population projected to live in urban areas by 2050*.

US Army War College. (2019). *A tale of two cities: The future of urban warfare*. Strategic Studies Institute.

United States. Joint Chiefs of Staff. (2002, September 16). *Doctrine for joint urban operations* (Joint Publication 3-06). Defense Technical Information Center. https://apps.dtic.mil/sti/tr/pdf/ADA434214.pdf

Wagner, B. (2019). Liable, but not in control? Ensuring meaningful human control over collaborative robot systems. *Policy and Society*, 38(1), 93–111.

Walsh, T. (2018). *2062: The world that AI made*. La Trobe University Press.

Weil, C., Bibri, S. E., Longchamp, R., Golay, F., & Alahi, A. (2023). Urban digital twin challenges: A systematic review and perspectives for sustainable smart cities. *Sustainable Cities and Society*, *99*, 104862. https://doi.org/10.1016/j.scs.2023.104862

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Crown.

Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.