Weaponizing Firmware, Cyberwarfare and Battery Management Systems: 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: As the Internet of Things (IoT), which is made up of "smart" devices, expands, in the cyber security space issues arise because cyber security which has traditionally focused on data privacy and service availability. However, a critical and under-analyzed threat vector lies in the weaponization of firmware to inflict kinetic physical damage on battery powered devices and battery management systems. This research analyzes the technical reality of manipulating Battery Management Systems (BMS) in civilian devices. By overriding safety protocols and de-throttling thermal limits, attackers can induce thermal runaway in lithium-ion batteries. This process effectively converts smartphones, laptops, and electric vehicles into incendiary devices. There is a reason why BMS security matters: The BMS directly governs safety limits; malicious interference could lead to device failure and fire risk, or grid instability when scaled. Modern connected devices increase the "attack surface" for cyber warfare via telematics, mobile apps, cloud APIs, and service diagnostics. Key risk categories (without operational details) include but are not limited to: Supply chain and tampering with components/firmware, insecure third-party libraries. There are issues related to Firmware/boot including unsigned updates, insecure bootloaders. With communications (Comms) there are weak or missing authentication on CAN or diagnostic interfaces; replay or spoofing risks. Issues with applications include Cloud/app weak API/auth controls, insecure mobile app backends. There are also Safety/security co-engineering gaps when functional safety (e.g., ISO 26262) and cybersecurity (e.g., ISO 21434) are not jointly considered. This paper explores the specific firmware vulnerabilities that allow for voltage manipulation and the bypass of hardware cut-offs for devices requiring batteries. Beyond the technical mechanics of batteries, we examine the ethical and legal implications of this "dual use" technology. This is where consumer electronics can be remotely triggered to cause fires or explosions. We argue that the potential for physical harm necessitates a reclassification of firmware vulnerabilities in power regulation modules, moving them from standard cybersecurity concerns to issues of public safety and kinetic warfare. This analysis will conclude with an ethical and anticipated ethical analysis of BootROM code when it is used in support of battery powered devices in cyberwarfare.

Keywords: Cyber-kinetic warfare, Battery Management Systems (BMS), Firmware weaponization, Anticipatory Technology Ethics (ATE), Dual-use technology, Thermal runaway, BootROM vulnerabilities, IoT security

1. Introduction

The paradigm focus of cybersecurity has been on preserving privacy for users' data and on the protection of the ability of users to access services in cyberspace. Significant resources are dedicated to engineering and implementing cybersecurity controls that enhance the security of users' operating systems and prevent unauthorized access to the data in these systems by hackers. Historically, this approach has been asymmetrically oriented toward protecting virtual infrastructure, neglecting to adequately address another area of the threat landscape: the exploitation of embedded firmware. The weaponization of this firmware allows attackers to execute kinetic attacks, causing users to suffer physical harm and property damage through malicious hardware manipulation (Donnelly & Wilson, 2026; Taddeo, 2012).

The potential and very real threat of cyber-kinetic warfare directed towards battery powered devices must now also be included as part of the bigger picture when defining cybersecurity. Cyber-kinetic warfare is currently an evolving theatre of operation in which digital breaches into information or operational systems go beyond merely manipulating the virtual world and will, in fact, cause actual physical destruction to the end-user of devices that have been compromised. The purpose of this research project is to highlight the technological realities of the modifications that can be made to battery management systems (BMS) in civilian electronic devices. Attackers can compromise the operational effectiveness of batteries in electronic devices that operate with lithium-ion batteries by overriding safety protocols related to the operational effectiveness of BMS. The result is the release of uncontrolled energy from lithium-ion batteries and, therefore, the deliberate and intentional cause of a thermal runaway condition can occur which, in turn, can result in the use of consumer technology as remote-detonation devices (Wang et al., 2023).

The BMS's security is essential for regulating the ultimate physical safety of the system's firmware/hardware. Should a malicious hacker attack firmware, it will not be just a case of lost data from the crashing of the program

but also multiple instances of catastrophic failure, risking the integrity of the entire unit and causing grievous injury or death when the attack reaches a large enough segment of interconnected smart systems. The increase in connected devices has greatly increased the attack surface related to all the devices due to the use of telematics, mobile applications, cloud APIs, and OTA diagnostic solutions. This paper examines different firmware vulnerabilities identified to exist across distinct risk categories defined as tampering via the supply chain, boot sequence, unauthorized communication interface access, and poor cloud controls that can facilitate manipulation of power generated by the device and allow overruling of safety cutoffs in battery powered devices and the IoT. Beyond the technical implications, this paper will also examine the ethical and legal implications of dual-use technology and why the physical safety ramifications must define the way firmware vulnerabilities associated with power regulating devices are classified. Firmware vulnerabilities associated with power regulating devices should be redefined and repositioned from standard computer cybersecurity to considerations that need to be perceived as urgent matters of public safety and warfare. The final section of this paper will include an ethical and ATE analysis of BootROM firmware code used to further the agenda of countries using nation-state sponsored cyberwarfare against other nation-states.

2. Technical Issues

To evaluate the ethical issues and strategic risks associated with the potential for firmware weaponization, requires dissecting the technical architecture of the Battery Management System (BMS) and identifying the appropriate attack vectors that can lead to the exposure of the system. Many of today's IoT (Internet of Things) endpoints and Electric Vehicles (EVs) have highly sophisticated, multi-CPU based architectures that utilize a common power supply as their energy source. The numerous vulnerabilities built into these types of autonomously functioning subsystems fall into numerous categories of significant risk based upon battery powered devices and Battery Management Systems.

2.1 Battery Management Systems and Thermal Runaway

Lithium-ion batteries have become a dominant energy storage technology because they have high energy density. However, lithium-ion cells can only operate safely in a very narrow range of voltage and temperature—2.5V–4.2V (Gabbar et al., 2021). Battery management systems (BMS) are critical embedded systems that monitor the balance of cell voltage, State of Charge (SoC), internal temperature, and current flow to prevent unsafe physical conditions from forming. If these voltage and temperature limits are exceeded, the battery experiences "thermal runaway." Thermal runaway is an uncontrollable, explosive chain reaction that occurs when heat produced by self-heating exceeds the amount of thermal energy that can be dissipated through the battery's exterior (McKerracher et al., 2021; Schram & Tummonds, 2024). It begins with the breakdown of internal layers of the battery, and the rate of heating in the battery rapidly exceeds the rate of heat removal, leading to the melting of internal chemical separators and volatile off-gassing, resulting in high pressure jet fires and catastrophic explosion.

Targeting the BMS specifically are attacks that will digitally enable this state while bypassing any hardware cut-off protection. Attackers can create a kinetic effect by using low-level hardware interfaces to inject malicious configurations, changing the voltages on the supply line systemically, and then forcibly disabling thermal throttles. By manipulating this data, attackers can trick the system into incorrectly charging or failing to detect age-old fault conditions, which in turn guarantees either an explosion or a fire without notifying the user of what is happening (Wang et al., 2023).

2.2 Supply Chain Vulnerabilities

Kinetic threats are primarily based on the worldwide, highly opaque supply chain for IoT hardware; manufacturers and assemblers are now being attacked prior to shipment to consumers, with the introduction of tampered or otherwise altered hardware components and/or infected firmware either during setup of device or during the assembly of devices. There are thousands of widely known third-party libraries (open-source or proprietary) being used in a BMS's firmware to perform routine functions. If a widely adopted library for power management has an unaddressed vulnerability, that vulnerability will then be incorporated into millions of devices from multiple manufacturers, and attackers will have a common target that is exceedingly difficult to identify and remediate (Wetzels, 2017).

2.3 Firmware and Boot Sequence Risks

The boot sequence of a device determines whether the device's power regulation is secure. If the boot sequence is not secure, regardless of any subsequent security controls deployed, the security of the device will be

compromised. A key risk associated with boot sequences is the delivery of unsigned or invalidated firmware update files to devices. If a device does not authenticate the digital signature of an OTA update file with a cryptographic key, then an attacker could send a specially crafted firmware update file to the BMS of the device and change its safety parameters (Tsang, et al., 2022).

Additionally, insecure boot loaders provide another opportunity for an attacker to insert persistent malware into a device before it loads its operating system after the hardware has been initialized. Since there is no cryptographic trust in the device's hardware, this is how kinetic payloads are transferred to power controllers through the boot sequence.

2.4 Communication Interfaces: CAN Bus and Diagnostic Risks

The Battery Management System (BMS) interacts with other microcontrollers within Electric Vehicles (EVs) and industrial equipment through a network called the Controller Area Network (CAN) bus. The CAN bus was developed in the 1980s and was designed as a reliable alternative to previous forms of transmitting data within a vehicle, but it was not designed for security. The CAN protocol does not include native encryption or message-authentication mechanisms (Siddiqui et al., 2023). Due to this flaw in its design, there is a risk of severe replay and spoofing attacks against these systems.

Once an attacker has been able to compromise access to the vehicle's controller area network (the compromised system could be an infotainment unit, a malicious adapter attached to the vehicle's On-Board Diagnostics (OBD-II) port, or a compromised telematics unit), they can easily capture and inject fraudulent CAN messages. For example, an attacker could deliberately generate excessive numbers of CAN frames that contain fraudulent diagnostic messages. By doing so, they could force the BMS to overcharge the battery or ignore a thermal warning; thus, causing the battery to be physically destroyed, leaving the vehicle's layer 3 software services unable to prevent the physical destruction from occurring (De Vincenzi et al., 2026).

2.5 Cloud APIs and Mobile Application Backends

The ability for cloud infrastructure to provide the ability to manage devices is the last major attack vector. Consumers and grid operators use mobile applications and web dashboards to keep track of EV (Electric Vehicles) charging status, precondition cabin temperatures or manage battery energy storage. These applications use Cloud APIs to connect and communicate with the physical devices.

When manufacturers use weak API access controls, hard-coded authentication tokens, or insecure mobile application backends - they are providing a way for an attacker to go directly from the public internet to the physical Device Management System (BMS). Attackers regularly exploit cloud weaknesses and can send generic malicious commands to populate entire fleets of devices at once. A compromised API does not only place at risk one vehicle -- but also takes away the ability for that attacker to send out these commands to hundreds or thousands of connected batteries and control systems at the same time to initiate fast-charge movements and disable the cooling pumps creating localized grid collapse & mass kinetic events (Lin, 2019).

2.6 Safety and Security Co-Engineering Gaps

Historic engineering standards associated with these systems internationally have focused on physically protecting systems as one discipline and protecting them via cyber security in another separate discipline. This leaves a substantial, dangerous gap for any co-engineering efforts within the two engineering environments (Kim, 2020). As two examples of global engineering standards used by the industry, ISO 26262 - which establishes functional safety through engineering processes; and ISO/SAE 21434; which identifies necessary standards for engineering and for cyber security.

Functional Safety is a term established by ISO 26262 as a standard for guiding the safe engineering process to functional safety of automobiles through detailed engineering requirements based on the ASIL (Automotive Safety Integrity Level) classification system (Bastos et al., 2025). Inherently, ISO 26262 is developed under the assumption of the system being operated in a benign environment and does not account for the potential for a cyber-attack on the vehicle systems. Hence, ISO/SAE 21434 was created to establish global engineering guidelines for automotive cyber security (De Vincenzi et al., 2026). Because the BMS (Battery Management System) is critical to both functional safety and cyber security, the failure of manufacturers to co-consider and integrate the two engineering disciplines is a significant vulnerability for threat actors to exploit, thereby creating organizational structural gaps between validated safety test results and validations from cyber security vulnerability assessments (Siddiqui, et al., 2023).

3. Ethical Issues

The technical realities of manipulating BMS systems and the vulnerabilities in their supply chains pose significant ethical difficulties. The unaddressed hardware issues associated with these systems move digital risks from the theoretical realm to actual existential and kinetic threats, making civilian infrastructure capable of becoming weapons of war.

3.1 Dual-use Technology and the Kinetic Threshold

The main ethical dilemma involves the fact that modern power management firmware for electronic devices often serves dual purposes. For example, the same hardware and software designed to charge a consumer's laptop or manage power flow in an EV can also be altered remotely and used to create an explosion or fire. This creates a grey area between civilian use of technology and military munitions (Lin, 2019).

The emergence of cyber-kinetic capabilities has altered the ethical understanding of warfare (Taddeo, 2012). There are strict rules of engagement as outlined by Customary International Humanitarian Law (IHL) and various modern legal systems. Based on Rule 92 of the Tallinn Manual 2.0, a cyber operation will be considered a formal "cyber-attack" if it is reasonably likely to cause death/injury to people, or cause physical damage/destroy objects (Schmitt, 2017). A digital payload used to ignite an electric vehicle parked in a civilian garage is the same as a kinetic incendiary strike from an ethical and legal perspective. Because battery management systems (BMS) have an inherent capability of dual use, it is almost impossible to apply the concepts of distinction (separation of military versus civilian targets) and proportionality when deploying cyber-kinetic weapons.

3.2 Reclassifying Firmware Vulnerabilities

The cybersecurity industry and regulatory authorities continue to evaluate firmware vulnerabilities as traditional data security and intellectual property problems. Because of the potential for directly harming individuals, a complete and fundamental reclassification of firmware vulnerabilities in power regulation modules to "immediate public safety and kinetic warfare" from the present standard cybersecurity concerns is warranted. A BMS bug, an insecure bootloader and/or an unauthenticated CAN bus interface should be legislatively and ethically reclassified from being standard cybersecurity concerns to immediate issues of "public safety and kinetic warfare," requiring government-level controls, strict laws requiring mandatory patching, as well as increasing penalties for manufacturers that knowingly sell products with co-engineering safety issues. A vulnerable battery is as much a public safety issue as a defective gas line or structurally deficient bridge.

4. Case Studies

Theoretical vulnerabilities regarding thermal runaway and communication spoofing are concretely substantiated by a growing historical record of sophisticated cyber-kinetic attacks and academic vulnerability proofs.

4.1 BadPower and FANDEMIC: Exploiting Consumer Power Management

The "BadPower" attack method was publicly displayed by Xuanwu Labs' security researchers in 2020. They did this by maliciously tampering with the data transmission channel used to negotiate power delivery between a fast charger and an attached device, forcing the power brick to deliver a constant voltage significantly beyond the device's hardware tolerance for power consumption. Because of this, the internal thermal protections of the device could not keep up with the performance requirements, and the internal device components melted and eventually caught fire - this was accomplished without any actual hardware manipulation (Xuanwu Labs, 2020).

Going further, the 2022 NDSS Symposium on Networked and Distributed Systems presented the FANDEMIC vulnerability framework. The researchers demonstrated that by deploying maliciously modified firmware to a power management integrated circuit (PMIC), they could modify the output of the PMIC voltage. By shifting the operational voltage by only 0.1V, a critical reading error was induced in physical sensors connected to the PMIC and thus proved that maliciously modifying power sources can cause critical logic circuit failures in cyber-physical systems without overtly causing a voltage spike (Tsang et al., 2022).

4.2 TRITON/Trisis Malware: Industrial Sabotage

In 2017, it was made clear by the TRITON malware incident that state actors were willing to use malicious means to bypass physical safety controls. The TRITON malware was deployed to the petrochemical plant and targeted the SIS (Safety Instrumented System), which is an autonomous computer that initiates an emergency mechanical shutdown of the equipment in all situations that may compromise safety. Attackers inserted malicious binaries

into the controller's active memory to blind the safety system permanently, ultimately enabling the plant to build pressure to a critical state and cause a catastrophic explosion (Federal Bureau of Investigation / CISA, 2022). The TRITON malware showed that threat actors have demonstrated both the technical capability and moral will to bypass physical safety measures through manipulation of embedded firmware to create a catastrophic event.

4.3 The Jeep Cherokee Exploitation: Telematics and CAN Bus Weaponization

In 2015 the remote, zero-click hacking of a Jeep Cherokee by Charlie Miller and Chris Valasek highlighted the kinetic risk of an unauthenticated link to the vehicle. Exploiting a vulnerability of Uconnect, the vehicle's cellular connected infotainment (telematics cloud) system, they accessed the system, bypassed an internal gateway allowing them to upload an unsigned maliciously modified firmware image to the V850 microcontroller (boot/firmware validation failure). By doing so they were able to pivot to the vehicle's unencrypted Controller Area Network (CAN) and inject spoofed diagnostic frames that provided them with remote physical access to the vehicle's steering, cruising transmission, and braking systems at highway speeds (Miller & Valasek, 2015). Thus, Miller and Valasek have provided definitive evidence that a cloud to hardware infection chain can result in immediate lethal kinetics to civilians.

4.4 MadIoT: Cloud APIs and Scaled Grid Instability

Individual device manipulations are extremely dangerous, but malicious actors may exploit Cloud API capabilities to expand cyber-kinetic attacks to the infrastructure level. Princeton research in 2018 introduced "MadIoT" (Manipulation of Demand via IoT) solutions for how an attacker could weaponize a vulnerable cloud back end that provided insufficient controls over API utilization and create regional power grid destabilization. Using a large fleet of vulnerable high-wattage consumer IoT devices (e.g. smart HVAC systems, EV chargers, home battery storage) as a compromised coordination of synchronized botnets, an attacker could execute a simultaneous command issued through cloud API to turn on or off all of the high-demand regulators, creating artificially induced massive frequency instabilities and line failures (Soltan et al., 2018). The research demonstrated that without co-engineering functional safety and cybersecurity, the aggregate of vulnerable internet-connected power modules could be aggregated into a weapon of mass disruption that has the potential to trigger widespread blackout events.

5. Anticipatory Ethics

Anticipatory Ethics is a future oriented ethical framework that studies potential ethical issues that arise from new and emerging technologies before they are fully integrated into society. As defined by Phillip Brey, Anticipatory Technology Ethics (ATE) requires that we move beyond reactive judgements about the effects of technologies after an event has occurred to a proactive forecasting of the dangers that these technologies pose. In order to properly address the integration of kinetic cyber threats into basic infrastructures, including individual vehicles and a macro-level power grid, a reactive approach is inadequate. The prompt installation of non-transparent power systems and unsecured communication systems requires proactive use of Anticipatory Ethics (Brey, 2012).

5.1 The Anticipatory Technology Ethics Framework

The Anticipatory Technology Ethics (ATE) framework provides a clearly structured way of analyzing technology's ethical impacts at the research and development (R&D) stages. It provides a method by which to examine and try to predict and mitigate any potential impacts on society by performing an ethical analysis of technology across three levels: Technology Level (the inherent properties of the technology), Artifact Level (the specific artifact that incorporates the technology, e.g., EV Battery Management System), and Application Level (the overall impact of that technology as it relates to scaling its application in broader society, e.g., aggregate grid load) (Brey, 2012). The ATE framework forces engineers and policy makers to formally acknowledge both the positive and negative uses of their designs from the very beginning. If engineers applied the ATE framework to their design of cloud APIs and CAN Buses prior to development, they could have anticipated the vulnerabilities of both the Jeep Cherokee and the MadIoT case studies and architecturally designed them out prior to putting civilian populations at risk (Miller and Valasek, 2015; Soltan, et al., 2018).

5.2 Ethical Analysis of BootROM in Cyberwarfare

Examining the foundational hardware under the lens of an ATE Framework reveals a massive unresolved ethical issue at the Base Layer, specifically about how BootROM Code (the first executed piece of code after the processor receives power from the device) is used in state-affiliated cyber warfare by the armed forces to engage in boot-level attacks. Unlike conventional applications, BootROM code is built to be unchangeable in nature —

it is truly embedded into the silicon of the microprocessor during production and can only be modified through physical means by either the end-user, the hardware manufacturer, or the operating system. It is the ultimate "Hardware Root of Trust" for confirming the integrity of digital signed images of Boot Loaders and the Operating Systems that run software on the device.

The use of BootROM, from the ATE point of view, is ethical because it is a permanent piece of hardware. Nation-state actors or intelligence agencies who find a vulnerability (or require it when they are put on the BootROM) can use it, as well as exploit that vulnerability, as a permanent, unpatchable way to access the processor associated with the BootROM. In a cyberwarfare scenario, gaining access to the BootROM allows the attacker access to the device at a level deeper than the safety measures in place for that device. An attacker able to exploit the BootROM may also be able to intercept the boot chain process, install signatureless malicious firmware (as seen in an exploited Jeep), and can run information from a BMS program (Battery Management System), causing the BMS program to induce an overheat condition, while sending false telemetry data back to the user and to the cloud API. Finally, compromising the BootROM will ensure that any infected device, powered by the same power sources as regular devices, utilized within a large-scale IoT botnet (as modelled in MadIoT) cannot be sanitized through a factory restore or receive standard over-the-air patches, creating an everlasting grid instability-based weapon embedded in a person's home.

From an ethical perspective, a nation state carrying out cyberwarfare through the use of BootROM exploits is in serious violation of the principle of proportionate use of force and that innocent people must not be harmed by the military use of these types of exploits. The code that is used in BootROMs is the same for all chipsets, so when a state actor uses an exploit against a military adversary, the state actor is also going to use it against civilians who are using the same type of equipment. Therefore, when state actors hoard BootROM vulnerabilities, rather than disclosing those vulnerabilities to the hardware manufacturers for future silicon revisions, they are ethically compromising the core safety of global civilian infrastructure by effectively turning consumer electronics into unpatchable munitions.

6. Recommendations

The cyber threats posed by kinetic warfare through power management manipulation and exploited IoT will require the industry to shift to verifiable architectural enforcement from the current reactive software patching model. This will involve multiple approaches involving trust in the hardware, engineering paradigms, communication protocols and supply chain integrity.

6.1 Hardware-Level Cryptographic Trust

All manufacturers must be legally obligated to establish strict, immutable hardware roots of trust. Furthermore, BootROM code must undergo extensive third-party auditing on a continuous basis before it is manufactured into silicon; this will prevent the creation of a sufficient number of unknown, state-sponsored backdoors that cannot be patched. In addition, all firmware updates should require cryptographic signature validation that is hardware-enforced to block the injection of malicious payloads. Products should be developed so that when a cryptographic signature cannot authenticate any portion of the boot sequence, the Battery Management System goes into a secure, physically separated state and prevents thermal runaway; instead of continuing to run in an operationally insecure state.

6.2 Unified Safety-Security Engineering

The automotive industry and the IoT space need to move away from siloed thinking that treats ISO 26262 (functional safety) and ISO/SAE 21434 (cybersecurity) as separate compliance checklists (Bastos et al., 2025). The industry needs an integrated Cybersecurity Management System. This integrated approach will ensure that threat models consider the kinetic outcomes of both intentional BMS manipulation and aggregated cloud API abuse. Engineering teams must perform joint Threat Analysis and Risk Assessments where cybersecurity engineers will be required to demonstrate through legal documentation that a digital attack cannot physically disable the safety cut-offs created by functional safety engineers.

6.3 API and In-Vehicle Network Authentication

Electric vehicle and energy storage systems' communications interfaces should have strict regulatory compliance. Therefore, all messages sent across the internal CAN bus (the communication interface) of electric vehicles and energy storage batteries should be cost effectively authenticated with the use of strong cryptography to protect against spoofing of diagnostic frames (Miller & Valasek, 2015). Because of the trust-based nature of the legacy CAN bus, manufacturers must logically and physically separate their CAN networks

(creating isolation within the communications network) from their electric vehicles' telematics and infotainment units (which communicate with the internet) and the microcontrollers that help regulate battery power. In addition to the above separation of the networks, strict multi-factor/threshold authentication and anomaly detection/rate limiting need to be enforced for all Cloud APIs communicating with the physical power controllers to eliminate the risk of synchronized Botnet attacks on the power grid (Soltan et al., 2018).

6.4 Supply Chain Verification and Liability

Overall, the international regulatory framework must address the global hardware supply chain's lack of full transparency. Governments must enforce strict liability on manufacturers that include unverified and/or insecure third-party libraries into the critical power management firmware. A Software Bill of Materials (SBOM) and a Hardware Bill of Materials (HBOM) must be required on any device capable of storing or routing lethal amounts of kinetic energy. This will enable security researchers and grid operators to quickly identify, audit and isolate vulnerabilities prior to being weaponized at the national level through forcing manufacturers to list with full transparency all the materials and open-source software libraries used in their devices.

7. Future Work

The rapidly increasing global move to electric power for transport and the creation of large-scale battery systems will greatly expand the potential for hackers to obtain access. A key area of future research, both by academia and industry, must focus on the development of embedded AI (Artificial Intelligence) and ML (Machine Learning) that uses the CAN bus to create real-time anomaly based intrusion detection systems (IDS) that can detect and mathematically eliminate fake diagnostic frames before they can be accepted by the BMS (Battery Management System). Similarly, continuing to conduct extensive R&D (Research & Development) into grid level defensive orchestration that can automatically detect and mitigate synchronized power drops by large IoT botnets will be of the utmost urgency. Lastly, ongoing academic investigation into the complicated challenge of integrating post-quantum cryptography into BootROMs and legacy PMICs (Power Management Integrated Circuits) will be essential to prevent advanced threat actors from implementing "harvest now, decrypt later" plans against the new smart grids and energy systems being enabled by clean energy.

8. Conclusion

With the growth of IoT technologies and their connectivity, the traditional focus of cybersecurity regarding data privacy needs to shift to a proactive approach to prevent loss, economic damage, or catastrophic physical harm from kinetic attacks. The potential of commercial Battery Management Systems (BMS) to launch kinetic attacks by taking advantage of archaic vulnerabilities in commercially available electronic components illustrates the limitations of modern physical infrastructure. Exploiting supply chain gaps (e.g., unverified CAN bus communications), API/Cloud-based communication vulnerabilities, and long boot sequences, attackers can bypass the inherent safety limit cuts on all types of inventory and products to cause thermal runaway, creating widespread use of consumer goods as means of creating exploding fires. As seen in recent cases where telematics and cloud systems have functioned as weapons, these exploits can quickly move beyond individual vehicles being hijacked to precipitating mass blackouts within entire regions.

We need to change many things we think about governing technology. We must close the gaps between functional safety and cybersecurity for good. Firmware vulnerabilities that affect power systems need to be classified not only as software bugs but also as critical public safety issues. An anticipatory ethical assessment on the foundational hardware called immutable BootROM code demonstrates that the accumulation of unpatchable silicon vulnerabilities for cyberwarfare by nation-states creates an unacceptable risk to the lives of civilians. BootROM vulnerabilities allow nation-states to bypass high-level software defenses and ultimately compromise the hardware root of trust so the continued use of BootROM exploits by nation-states creates sustained dual-use weaponry out of civilian devices. Until the enactment of strong legally enforced hardware-based cryptographic trust and unified safety-security frameworks, the interconnected infrastructure of the digital age remains an unconstrained and kinetic threat to international cyber security and stability.

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

Bastos, S., Branco, K. C., & Oliveira, A. (2025). Bridging the Gaps: A Comparative Analysis of ISO 21434, ISO 26262 and Machine Learning in Autonomous Vehicles. Journal of Cybersecurity and Privacy.

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

De Vincenzi, M., Bodei, C., & Matteucci, I. (2026). When AI takes the wheel: AI-defined vehicles principles and pitfalls. *Frontiers in robotics and AI*, *13*, 1770121.

Donnelly, N., & Wilson, R. (2026). Malinformation, Deepfakes, and Cyber Warfare: Ethical and Anticipated Ethical Issues. Proceedings of the 21st International Conference on Cyber Warfare and Security (ICCWS), 21(1), 75-82.

Federal Bureau of Investigation / CISA. (2022). TRITON Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems (ICS). CISA Alert.

Gabbar, H. A., Othman, A. M., & Abdussami, M. R. (2021). Review of battery management systems (BMS) development and industrial standards. Technologies, 9(2).

Kim, S. (2020). Safety and Security Co-engineering in Automotive Systems. ScitePress.

Lin, H. (2016). Governance of Dual-Use Technologies: Theory and Practice. American Academy of Arts & Sciences.

McKerracher, R. D., Guzman-Guemez, J., Wills, R. G., Sharkh, S. M., & Kramer, D. (2021). Advances in prevention of thermal runaway in lithium-ion batteries. Advanced Energy and Sustainability Research, 2(5), 2000059.

Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015(S 91).

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

Schram, & Tummonds. (2024). Causes and Prevention of Thermal Runaway in Lithium-Ion Batteries. Electric Power Research Institute (EPRI).

Siddiqui, F., Khan, R., Yengec Tasdemir, S., Hui, H., Sonigara, B., Sezer, S., & McLaughlin, K. (2023). Cybersecurity Engineering: Bridging the Security Gaps in Advanced Automotive Systems and ISO/SAE 21434. Queen's University Belfast.

Soltan, S., Mittal, P., & Poor, H. V. (2018). BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. 27th USENIX Security Symposium (USENIX Security 18), 15-32.

Taddeo, M. (2012). Information Warfare: A Philosophical Perspective. Philosophy and Technology.

Tsang, R., Joseph, D., Wu, Q., Salehi, S., Carreon, N., Mohapatra, P., & Homayoun, H. (2022). FANDEMIC: Firmware Attack Construction and Deployment on Power Management Integrated Circuit and Impacts on IoT Applications. Network and Distributed System Security (NDSS) Symposium.

Wang, G., et al. (2023). Critical review and functional safety of a battery management system for large-scale lithium-ion battery pack technologies. MDPI Energies.

Wetzels, J. (2017). Broken Embedded Patch Management and the Forever Day. Black Hat / DEF CON.

Xuanwu Labs (Tencent). (2020). BadPower: Hacking fast charging firmware to melt devices. Black Hat Security Conference Presentations.