НАЦИОНАЛНА СИГУРНОСТ
NATIONAL SECURITY

DELEGATING CYBER DEFENSE TO ALGORITHMS: THE LEGAL BOUNDARIES OF AUTONOMOUS RESPONSE IN BULGARIA

Vladimir Babanov
South-West University "Neofit Rilski"
https://doi.org/10.70300/NEXH2197

Abstract: *The article examines the legal implications of autonomous response mechanisms in the Bulgarian cyber defense system. It analyzes Bulgaria's legal framework and observes it into the broader context of NATO and EU's strategic documents. The article defines and studies the legal viability of autonomous cyber response, highlighting how automated defensive actions challenge existing legal standards. The evolution of Bulgaria's cyber defense posture is documented, beginning with early cyber defense strategies and through to the most recent alignment of the EU directives and NATO requirements. The discussion reveals that the Bulgarian law does not provide specific legal authorization for automated counter-measures in the case of cyber-attacks. The lack of legal authorization creates theoretical and compliance issues. The article concluded that while the national law of Bulgaria provides a comprehensive base to address cybercrime and protect critical infrastructure, there are challenges to incorporate autonomous cyber responses into existing legislation. It is based on the clear presumption that development of any strategy requires compatibility with the international obligations of the country.*
Keywords: *cyber defense; autonomous response; artificial intelligence; legal framework; Bulgarian legislation*

INTRODUCTION

Cyber defense has become an essential aspect of national security. With the rise of autonomous response systems, utilizing artificial intelligence (AI) for detecting and countering cyber threats without human intervention, nation-states seek to develop ways to defend their networks at machine speed. However, the development of technology complementing cyber defense is evolving ahead of existing legal frameworks and EU's policy for investment in cyber defense is a broad attempt to reverse this tendency. Still, there is little clarity regarding the legal authorization of these types of activities. The disconnect between developing technologies and established legal frameworks is evident in Bulgaria as the country seeks to expand its cyber defense capabilities, while maintaining the rule of law and guaranteeing human rights.

The circumstances in Bulgaria represent the dilemma of how to facilitate the national legislature to the emerging practices in cyber defense. Bulgaria has established an internal legal foundation for cybersecurity via the Updated National Strategy for Cybersecurity, the Cybersecurity Law and the Criminal Code, which source from EU directives. At present, due to delay in implementing the NIS2 Directive, Bulgaria's cyber defense system is based on Cybersecurity Act of 2018 and the NIS1 Directive, which establishes the nation's apparatus for overseeing the security of networks. Additionally, as a NATO ally, Bulgaria is integrated into alliance cyber strategies and engages in joint exercises and information-sharing (SHAPE Public Affairs Office 2025).

Evidently, there are still unknowns to whether the Bulgarian legislature allows for more proactive or automated cyber responses to threats. Such unknown is the question: would an AI-enhanced defense system be legally cleared to act autonomously against an ongoing threat? Additionally, the problem for legal accountability in case an autonomous countermeasure results in unintended damage remains open. This article addresses such questions by assessing the relevant legal framework of the country in relation to autonomous cyber operations.

METHODOLOGY

This paper follows an academic approach to describe Bulgaria's legal and institutional framework, covering national laws under the impact of EU and NATO agendas. Following the description of the legal and institutional framework, a definition of autonomous cyber response is derived to clarify the terms used throughout the paper. The development of Bulgaria's cyber defense posture within the context of EU and NATO is approached in a holistic manner. The empirical data, gathered by reviewing and analyzing laws, codes and relevant literature, illustrates the legal specifics and theoretical gaps in the Bulgarian law for potential areas of ambiguity or lack of alignment with autonomous response capabilities. The Discussion section fuses the findings while the Conclusion offers final thoughts on reconciling the technological possibilities of autonomous cyber response with the legal and ethical imperatives in Bulgaria's cyber defense.

DISCUSSION

Defining "Autonomous response"

Autonomous cyber response refers to the process of automated systems performing various cyber defense functions. Conducted by a blending of software, hardware and AI, the autonomous actions might include identifying and blocking malicious traffic, isolating an attacker's access to a network, or response to a cyber-attack without human involvement in the decision-making process. Autonomous cyber response should hold a degree of automation sufficient enough for the system to operate independently of human presence. The defining characteristic of autonomous response systems is their ability to monitor circumstances and execute adequate countermeasures with speed and agility that exceeds the ability of humans to respond.

Legally centered literature distinguishes "passive" automated responses to cyber threats from "active", that may include offensive countermeasures against an adversary. While there has been increasing discussion on active cyber defense in Europe, the legal and political circumstances for their use remain poorly defined (Bendiek & Bund 2024). They emphasize on European cyber defense postures that delegate responsibility to the states to create normative frameworks regarding the deployment of active cyber defense measures. The aim is avoidance of unregulated or disorganized uses of active cyber defense, which would be likely to result from undefined authorities. A major concern with respect to the use of cyber countermeasures is the compliance of the actions with established principles of international law, including sovereignty, due diligence, and proportionality. For example, Germany's 2023 National Security Strategy explicitly ruled out "hackback" as a means of defense, stating that "there are high legal hurdles" to using this type of measure, and that reliable attribution of an attacker is necessary prior to taking action (Bendiek & Bund 2024). This provokes a broader caution in Europe regarding crossing the line between defensive and offensive operations in cyberspace.

A key distinction must be made between autonomous defensive cyber response and offensive hacking. Organizations today often employ automated cyber defenses as most recognize their legitimacy and legality, since they only occur inside an organization's own network. However, the focus of the discussion is on more comprehensive and autonomous cyber defense measures, which may involve the use of cyber defense techniques that actively seek out attackers and pursue disruption of the source of an attack. In particular, when these measures are automated, they begin to approach what has been referred to as "offensive security". For example, an autonomous defense system might be capable of injecting a code to clog a server that has been identified as malicious for the Bulgarian infrastructure. While the intention behind such action may be legitimate, the manner of its implementation raises legal concerns if it were to operate across networks outside the jurisdiction of the Bulgarian government.

From a military perspective, autonomous cyber capabilities may be seen as similar to a sentry system that alerts authorities in case of an attack and takes active steps to counter it. Researchers at NATO have noted that the term "autonomy" in the context of cyber operations can apply equally to both defensive and offensive tools (Liivoja, R. et al. 2021). The mentioned level of autonomy can reside in three different areas: target selection to counter, methods on how to counterattack or iso-

late, and effect on the parameters within which the system operates to achieve a desired outcome. However, fully autonomous cyber weapons may be able to replicate themselves across a network and disable enemy systems on their own or go rogue, and examples of such autonomous weapons include Stuxnet (Scharre 2018).

However, the focus of this examination remains centered on national cyber defense, specifically autonomous responses employed by a nation-state or its critical infrastructure in order to protect itself against cyber-attacks. Importantly, complete autonomy in cyber defense systems does not exist, rather there exists varying degrees of human oversight. Systems may require a human to approve suggested courses of action (human-in-the-loop), may provide a human with monitoring and intervention capabilities, or may strive for completely independent action. As the degree of autonomy increases, so too does the challenge to existing legal frameworks that strongly assume the existence of human agency. Therefore, as part of the current examination, the existing Bulgarian law is assessed.

Legal and institutional context in Bulgaria

The legal system in Bulgaria primarily regulates cybersecurity at the national level via its general criminal laws, and special laws. The Bulgarian Criminal Code has been regulating the key cybercrimes since 2005, when Bulgaria signed the Budapest Convention on Cyber Crime (Council of Europe 2001). The Criminal Code specifically forbids illegal access to a computer systems and data, attacks on critical infrastructure, or systems interference as well as other cybercrimes (Criminal Code: Article 319a-319e). The penalties for the unauthorized intrusion and other cybercrimes can result in prison sentences of up to 12 years, increasing to 15 years for compromise of national security or state secrets. These provisions suggest that private "hackback" or vigilante justice is prohibited in the cyber realm and is still perceived as a criminal offence. According to the Criminal Code, the defensive actions in cyberspace must be conducted within the law, which generally requires protective measures instead of offensive retaliation.

In 2018, Bulgaria passed the Cybersecurity Act to create a regulatory framework for the protection of network and information security. This Act transposes the European Union's (EU) NIS Directive (2016/1148) and therefore primarily addresses the resilience of vital infrastructure and digital service providers. The Act assigns tasks and mechanisms for inter-agency cooperation rather than the execution of offensive cyber operations. The Ministry of e-Governance is designated as the national competent authority and single point of contact for cybersecurity matters pursuant to this law (Geneva Digital Platform 2018) Under the Act, a multi-layered structure is created including Cybersecurity Council to coordinate high-level matters, a National Computer Security Incident Response Team (CERT Bulgaria) to handle operational incident response issues, and sectoral CSIRTs for critical sectors.

Essential services operators such as energy, transportation, banking, healthcare, etc., are required to implement security measures and report incidents quickly pursuant to the Act. While the Cybersecurity Act enhances an entity's readiness to defend itself, it does not authorize any form of "active defense" beyond an entity's own network. In fact, cyber incidents that may be criminal in nature are to be referred to law enforcement, not to defense authorities. The Act stipulates that the cybercrime unit of the Ministry of Interior is to be consulted with during investigations of incidents that may constitute a crime.

Bulgaria's defense establishment has also undergone changes to address cyber threats. The Law on Defense and Armed Forces was amended in 2021 to include a new Cyber defense Command as part of the Bulgarian Army. The creation of the Cyber defense Command, along with a Logistics Support Command, signifies that cyberspace is formally recognized as a domain of military action. The Chief of Defense now has control of the Cyber defense Command and has integrated it into defense planning and operations. However, in peacetime, the mandate of the Cyber defense Command is limited by law as the military cannot take action against cyber threats without certain legal thresholds, such as a state of war or emergency, being met or providing assistance to civilian authorities upon their request.

Bulgaria's law traditionally separates internal security, handled by the police and security

agencies under civilian law, from defense against external aggression, handled by the armed forces under defense-related laws and international conventions. Thus, the question for cyber defense arises as sophisticated cyber threats can often blur the distinction between internal and external or criminal activity and a breach in national security. At present, Bulgaria has not publicly defined rules of engagement for its Cyberdefense Command. Autonomous cyber response by the military, if any, would need to respect both domestic law restrictions and international legal norms.

Bulgaria's cyber defense is shaped by its commitments to the EU and NATO. EU law is the underlying structural framework for Bulgaria's national cyber defense and EU initiatives guide predominantly Bulgaria's legal approach. The NIS Directive, the future NIS2 Directive updates for Bulgaria, and the EU's 2022 Cyber Defense Policy, call on member states to develop full-spectrum cyber defense capabilities, including active cyber measures, in a coordinated manner (Bendiek & Bund 2024). The Council of the EU in 2023 stressed that such measures must remain "defensive" in character, and the decision and responsibility for implementing them rests with each state. Therefore, Bulgaria must develop its own policy on active cyber defense, ensuring that any actions taken comply with EU principles and with the UN-endorsed norms of responsible state behavior in cyberspace. Furthermore, as an EU member state, Bulgaria participates in ENISA's programs and can partake in joint cyber drills or the Cyber Rapid Response Teams initiative, that is a voluntary initiative among some EU states.

These mechanisms improve Bulgaria's capability to respond to cyber threats, but do not supersede Bulgaria's law regarding the use of force or law enforcement.

Membership in NATO is yet another dimension of the context in which Bulgaria adopts its laws. NATO recognized cyberspace as a domain of operations in 2016 and allies agreed to enhance their collective cyber defenses. As a member of NATO since 2004, Bulgaria has aligned its policies with the Alliance's Cyber Defence Pledge and Strategic Concept. NATO's 2022 Strategic Concept describes cyberspace as "continuously contested", requiring preparation for defense across the spectrum of peace, crisis, and conflict. In July 2023, NATO approved a new cyber defense policy to enable seamless civil-military cooperation in respective situations.

From a practical perspective, this encourages NATO members to enhance coordination between their civilian cybersecurity organizations and their military cyber organizations at all times. In fact, Bulgarian officials emphasize that the armed forces, security services, and civilian agencies must work "side-by-side" to develop cyber resilience (Petrova 2025). Bulgaria also benefits institutionally from NATO resources by participating in Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. Bulgaria also hosts the NATO Crisis Management and Disaster Response Centre of Excellence in Sofia (Council of Ministers 2021). Participation in these centers of excellence provides Bulgaria with expertise on cyber defense and cyber law doctrines. NATO exercises such as Cyber Coalition test Bulgaria's ability to respond to large scale cyber-attacks in concert with its allies. The interoperability within the alliance is further developed by the NATO's Federated Mission Networking which is critical for cyber defence and Bulgaria is a part of it.

With the update of the Bulgarian national laws and strategies a key benefit is the establishment of a Cybersecurity Monitoring and Response Center assigned to the State Agency for National Security. Its function is monitoring of critical communications infrastructure resilience, cyber incidents and responding adequately when needed. In terms of legislation, Bulgaria is currently in the process of transposing into national law the European Union's NIS2 Directive (Directive (EU) 2022/2555). Amendments to the Cybersecurity Act are being drafted as part of a broader effort to expand the range of regulated industries and impose increased requirements for security and reporting on those entities. The new regulatory regime is expected to be implemented any time soon and foresees additional organizations to cybersecurity regulations, promoting further cross-border coordination. While NIS2 primarily addresses resilience and incident response, it also has an indirect impact on active defense through the elevation of capabilities to detect and respond to threats at an earlier stage. In such cases, an autonomous system would act in a preventative manner.

However, any offensive cyber response by Bulgaria in a real-world scenario would likely require political approval at the highest levels, and if executed as part of NATO, would require

consensus among allies. This comprises a difficult threshold that inherently restricts autonomous or unilateral cyber responses through its traditional chain of command. Therefore, Bulgaria's legal context for cyber defense includes criminalization of cyberattacks and a comprehensive cybersecurity governance framework focused on prevention, resilience, and incident response. The institutional arrangements for addressing cybersecurity overlap civilian organizations and the military in conjunction with the recommendations provided by the EU and NATO. What is absent is clear legal direction on autonomous or active countermeasures in cyberspace as it becomes a pressing issue with the AI development and adoption.

Legal uncertainties and gaps

Evidently, the Bulgarian cyber defense architecture is still in development and the possibility of a legal framework authorizing autonomous cyber response is not discussed yet. The gaps in the legal framework are both theoretical and practical. The next pages focus on several crucial gaps that need to be addressed for entertaining the concept of autonomous response in cyber defense.

The first one illustrates the lack of legal authority for offensive cyber operations. Neither Bulgarian cybersecurity nor defense legislation contain precise allowances for offensive cyber operations, whether conducted by humans or machines. There is no provision that permits an entity to "hackback" an attacker that has compromised their systems, even in self-defense. Such actions would likely fall within the scope of Article 319a of the Criminal Code or similar, putting the entity at risk of prosecution, just as the hackers would be. Bulgarian authorities, though, do have the power to conduct undercover technical activities with court order through legally regulated offensive means for the purposes of investigation.

However, these are limited to specific cases and do not provide blanket authorization for autonomous retaliatory actions. The Law on Defense and Armed Forces and the associated strategies detail plans for developing defensive capabilities to counter cyberattacks, but they fail to specify rules of engagement for taking offensive action against adversary computing resources through autonomous systems. In essence, Bulgarian law currently views cyber defense as protecting native systems, and pursuing cybercriminals through law enforcement and investigation. Preemptive or autonomous disruption of an external threat, therefore, exists in a gray area of legality.

The Bulgarian defense law explicitly grants authority for decision making to human officials. The status of the President as Commander-In-Chief, the Government, the Minister of Defense, and the Chief of Defense have been established for the use of force or active defense measures. For example, any deployment of military capabilities, presumably regarding cyber operations beyond Bulgarian networks, would require proper legal approval and likely parliamentary review if not regulated in NATO and EU's strategic documents. The existence of an autonomous cyber response system that could operate outside of Bulgarian networks would disrupt the chain of command.

Legally, delegating military responsibilities to a machine even partially is not regulated. However, in an allied nation, such as the U.S., the case has an answer through the Department of Defense's Directive 3000.09 Autonomy in Weapon Systems (US Department of Defense 2023). The Directive excludes cyberspace operations from the scope due to the complexity of creating legal regulation (Scharre 2018) that is non-existent at the moment. Hence, if the Bulgarian Cyber defense Command was using AI to counterattack in cyberspace, it would be operating in a policy void. A possible interim solution is that such a system must be overseen by a human command responsible for the initiation and consequences of the autonomous defense. In this context, the questions about the legal liability in such developments are numerous.

Autonomous responses could also blur the distinction between the pursuit of criminal justice and national defense. In Bulgaria, as in most countries, if an incident is attributable to state actors or constitutes a national security threat, agencies such as DANS and possibly the military would be engaged. However, the legal standards for escalating involvement by law enforcement or defense agencies in cyber incidents are not clearly articulated. In this grey area, a serious cyber incident would likely be addressed under the Law of measures and actions in a State Emergency or the Defense Act only if it exceeded certain impact thresholds. In addition, an autonomous system responding with counter-measures could involuntarily draw Bulgaria into an unauthorized use

of force on foreign systems. If the addressed incident proves to be a criminal case and as such- a matter to international cooperation, Bulgaria might be violating international treaties and laws.

As mentioned above, there is a key theoretical void in how Bulgarian law would assign accountability for the decisions by an automated AI system in cyber defense. In a presumable case, an autonomous response tool employed by the Bulgarian state identifies a cyber-attack on critical infrastructure and therefore automatically executes a script that incapacitates the attacking party's source. Consequently, the source turns out to be a legitimate server that had been spoofed by an attacker resulting in harm to a foreign business or a critical service. Such a scenario would raise many legal issues. Under the Bulgarian law, such actions are deemed responsible for damages suffered by the legitimate server owner and potentially criminally liable.

The EU's AI Act does not provide a basis for holding AI systems accountable. Instead, it provides a basis for human legal responsibility. In the context of Bulgaria, however, there is no specific legislation that addresses the use of AI in defense or security. Therefore, any autonomous action taken by Bulgaria in defense would be governed by existing laws that presume human purpose and control. This could result in a discouragement for the adoption of autonomous tools due to the associated legal risks. Alternatively, for the provider of the autonomous tool there is a potential legal gray area that might be exploited unethically.

Although the primary focus is on national law, Bulgaria's use of autonomous cyber responses intersects with its international obligations. If an autonomous cyber response by Bulgaria were to unintentionally harm systems of another state, it could be interpreted as a violation of sovereignty or as an unlawful use of force under international law. Bulgaria, as an EU member, endorses the 11 voluntary norms of responsible state behavior in cyberspace that were recognized by the UN (UN General Assembly 2021). However, if an autonomous counterstrike results in unintended consequences such as collateral damage, it may violate some of these norms too.

Additionally, if Bulgaria becomes a victim of a cyberattack, NATO's collective defense provisions could be invoked, but a response, including an autonomous one, would still require human political decision. In other words, while technology may automate certain parts of the response, the law and the international obligations do not foresee automation of war. The existing theoretical gap can be found in the lack of a conceptual or legal framework connecting low-level autonomous defensive mechanisms to higher level countermeasures.

The term "autonomous response" itself is undefined in Bulgarian legislation. Addressing the problem should begin with clearing the uncertainty around its meaning. For Bulgaria, defining this in law or strategy would be beneficial. The current National Cybersecurity Strategy (as updated through 2023) includes provisions for an "effective mechanism for rapid and coordinated response to large-scale cyber and hybrid attacks" (Council of Ministers 2021) and for the development of countermeasures to reduce the negative consequences of such attacks. However, the strategy does not mention offensive measures but the ambiguity can be viewed as a deliberate precautionary measure. Nevertheless, as Bulgaria develops new strategies, a clearer policy definition may become necessary. Gaps in definitions at the theoretical level could bring operational gaps in implementation.

Bridging the gaps and possible solutions

The development of Bulgaria's cyber defense showcases the difficulty of integrating modern, advanced technology into an established, legal and institutional framework. The prior analysis illustrated Bulgaria's progress in enhancing cyber defense under the rule of law. However, there is still considerable policy and legal work to be accomplished in terms of autonomous cyber-response if the government deems it necessary.

The analysis brings forward the need towards a reactive-only posture for cybersecurity to a more proactive posture, provoked by the pressing technology advancements. Recent legal framework trends in EU and NATO clearly demonstrate a shift toward anticipating and preventing cyber-attacks, rather than responding after their occurrence. For Bulgaria, this suggests a requirement for national legislation to explicitly permit the government engagement in proactive cyber defense activities. This does not necessarily mean the inclusion of autonomous response to attacks

but refinement of the legislation to reflect the current trends in technology should be considered. Any such provision would need to incorporate adequate checks and balances as clear criteria, human oversight, and compliance with international law. Importantly, if these actions are to be autonomous, then regulatory mechanisms must provide for human accountability to remain. A viable mechanism to accomplish this is to require a chain of command to approve or authorize the deployment of autonomous counter-measures to preserve human accountability.

NATO's emphasis on conducting operations throughout the spectrum provides Bulgaria the opportunity to develop doctrines for military assistance in large-scale cyber incidents short of war. An initial step would be to establish legislation or protocols between the civilian authority in charge of cybersecurity and the Ministry of Defense specifying the conditions and manner in which the Cyber-defense Command could assist in the event of a national cyber-crisis. Such protocols may provide specific details on when and how military cyber-units may utilize certain tools, including automated ones, to assist in containing and recovering from cyber-attacks under the direction of the civilian authority during times of peace. Establishing such formal relationships would eliminate uncertainty and ambiguity on role separation and how Bulgaria intends to conduct national cyber-defense.

A primary concern raised in the context of autonomous response is the possible balkanization of cyberspace with unaccountable algorithms. To mitigate, Bulgaria and similarly situated countries, could commit that any active cyber-defense measures employed would be defensive and proportionate. Enshrining such a commitment would be consistent with the normative principle of due diligence and responsible state behavior, and would provide a framework for domestic purposes. Hence, instead of focusing on autonomous counterattacks, Bulgaria could focus on employing autonomous containment.

Another factor frequently overlooked in the context of law is whether operators and decision makers have a sufficient level of competence to operate and direct autonomous cyber response systems. In order for the Bulgarian command to either authorize or rely on AI-based cyber response systems, they would need understanding of the systems' capabilities and limitations. Therefore, while Bulgaria may need to invest in technical capacity to train personnel to effectively operate AI-based cyber response systems, the capacity building itself should also be clear and legal in nature. Training programs should provide scenarios illustrating autonomous cyber response and teach how to assess such actions under both domestic and international law. The fact that Bulgaria has incorporated academic institutions into its cyber-exercise program, suggests that it can extend effort to include law academics and practitioners to facilitate simulation of decision-making in cyber-crises. Ultimately, this enables a body of professionals with understanding of both the technology and the jurisprudence associated with cyber defense.

Due to Bulgaria's membership in NATO and the EU, it is able to participate in shaping the evolving norms related to autonomous cyber defense. Through participation in NATO's CCDCOE and EU working groups, Bulgarian experts could contribute to the development of common definitions for concepts such as active defense, countermeasures, law enforcement activities and armed response in cyberspace. In addition to ensuring that Bulgarian national interests are represented, participation in these forums would also enable Bulgaria to advocate for a cautious, law governed approach to autonomous cyber defense.

The upcoming NIS2 Directive would increase the number of entities subjected to cybersecurity obligations in Bulgaria. Therefore, entities would need to implement more advanced security measures, some of which may utilize AI-based security solutions. Bulgarian regulators would need to prepare to provide guidance and assess the upcoming advanced security measures. Under the law, regulators may interpret provisions allowing for autonomous responses within the control of entities managing their own risk. Regulators may also encourage the use of automation for increased speed. However, regulators must ensure that internal autonomous responses do not become inadvertently offensive. For example, an overly aggressive endpoint security AI should not be allowed to "strike back" at foreign IP addresses unless authorized by competent authorities. Additionally providing guidance in implementing regulations of the Cybersecurity Act, amended to comply with NIS2, would be advisable.

CONCLUSION

The research has revealed the gap between what technology is capable of and what the law permits. The legislation should play a major role in regulating what benefits risk-countering associated with the use of technology. As part of the EU, Bulgaria has implemented relevant EU Directives and NATO strategies with relative success, envisioning the lagging NIS2 implementation. This has allowed the country to build institutions that boost the increase of cyber resilience and promote international cooperation. However, technology and threats continue to advance at a rapid rate. The next step in improving cyber defenses is to develop legislation that regulates systems capable of automatic responses to cyber incidents but in limited scope and always with human-in-the-loop.

The Bulgarian legislation currently follows a conservative approach according to automated processes. Presently, there is no legal provision for an AI to conduct independent counter-measures against hackers but its usage in certain activities is definitely an entertainable option. Therefore, the three key gaps identified in the research regarding authorization, accountability, and the overlap of defense and law enforcement functions, are not unique to Bulgaria, as the country's law-making must be in compliance with the rest of its allies in NATO and EU. Furthermore, addressing the gaps would require establishing clear boundaries and responsibilities regarding the deployment and usage of autonomous response systems. It is possible to deploy autonomous response systems, consistent with Bulgaria's existing legal obligations. For example, allowing the use of automated blocking or deception of incoming attacks is achievable and is unlikely to generate ethical controversy. Debating and defining whether and when active measures may be taken, including disabling an attacker's capabilities, is a complex task that could be undertaken in policy forums involving stakeholders.

The case of Bulgaria illustrates a problem that exists in many countries today. It consists of reconciling technological innovations in cyber defense with a commitment to legality and solidarity among allies. The debate of AI adoption on all levels of defense is persistent and urgent which means that the legislation would not avoid dealing with the matter in the future. By actively identifying and closing the gaps in the legal and theoretical frameworks, Bulgaria can establish a solid basis for integration of autonomous response capabilities into its cyber defense apparatus. The goal would be enhancement of cyber defense posture while maintaining the principles of accountability and state responsibility.

REFERENCES

BENDIEK, A.; BUND, J., 2024. Hardening Norms and Networks: Europe's Cyber Defence Posture. *Intereconomics*, *59*(4), pp. 198–203. [viewed 7 January 2026]. Available from: https://sciendo.com/2/v2/download/article/10.2478/ie-2024-0041.pdf

COUNCIL OF EUROPE, 2001. *Convention on Cybercrime, Budapest, European Treaties Series-185*. [viewed 7 January 2026]. Available from: https://rm.coe.int/1680081561

COUNCIL OF MINISTERS OF REPUBLIC OF BULGARIA, 2021. *Updated National Cybersecurity Strategy "Cyber-Resilient Bulgaria 2023"*. [viewed 7 January 2026]. Available from: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/BG_NCSS_2021_en %28draft translation%29.pdf

GENEVA DIGITAL PLATFORM, 2018. *Bulgaria's Cybersecurity Law*. [viewed 7 January 2026]. Available from: https://dig.watch/resource/bulgarias-cybersecurity-law

LIIVOJA, R.; VÄLJATAGA, A. (Eds.), 2021. *Autonomous cyber capabilities under international law*. NATO Cooperative Cyber Defence Centre of Excellence. [viewed 7 January 2026]. Available from: https://ccdcoe.org/uploads/2019/07/Autonomy-in-Cyber-Capabilities-under-International-Law_260619-002.pdf

PAUL, S., 2018. *Army of None: Autonomous Weapons and the Future of War* (W W Norton & Company 2018) 214–5; ISBN 0393608980. [viewed 8 January 2026]. Available from: https://ftp.idu.ac.id/wp-content/uploads/ebook/tdg/MILITARY%20PLATFORM%20DESIGN/Army%20of%20None%20Autonomous%20Weapons%20and%20the%20Future%20of%20War.pdf

PETROVA, P., 2025. *Defence Minister: Bulgaria Must Continue to Develop Cyber-defence Capabilities*, БТА. [viewed 8 January 2026]. Available from: https://www.bta.bg/en/news/bulgaria/1021735-defence-minister-bulgaria-must-continue-to-develop-cyber-defence-capabilities

SHAPE PUBLIC AFFAIRS OFFICE, 2025. *Exercise Cyber Coalition, NATO's flagship Cyber Defence exercise, concludes in Estonia*. [viewed 7 January 2026]. Available from: https://shape.nato.int/news-archive/2025/exercise-cy-

ber-coalition--natos-flagship-cyber-defence-exercise--concludes-in-estonia
THE US DEPARTMENT OF DEFENSE, 2023. *DOD DIRECTIVE 3000.09 AUTONOMY IN WEAPON SYSTEMS*. [viewed 8 January 2026]. Available from: https://media.defense.gov/2023/Jan/25/2003149928/-1/-1/0/DOD-DIRECTIVE-3000.09-AUTONOMY-IN-WEAPON-SYSTEMS.PDF
UN GENERAL ASSEMBLY. *Group of Government Experts on Advancing responsible state behaviour in cyberspace in the context of international security*, A/76/135, 14 July 2021, paragraph 15; UN General Assembly, Open-ended working group on developments in the field of ICTs in the context of international security, A/75/816, 18 March 2021. [viewed 8 January 2026]. Available from: https://docs.un.org/en/A/80/257
ZAKON ZA OTBRANATA I VAORAZHENITE SILI NA REPUBLIKA BULGARIA, obn. DV, br. 35 ot 12 may 2009 g., izm. i dop. DV, br. 100 ot 25 noemvri 2025 g., popr. DV, br. 101 от 27 noemvri 2025 g. [viewed 7 January 2026]. Available from: https://www.lex.bg/en/laws/ldoc/2135631954
NAKAZATELEN KODEKS, chlen 319a-319e, obn. DV, br. 35 ot 12 may 2009g., izm i dop. DV, br. 100 ot 25 noemvri 2025g., popr. DV, br. 101 ot 27 noemvri 2025 g. [viewed 7 January 2026]. Available from: https://lex.bg/laws/ldoc/1589654529

ДЕЛЕГИРАНЕ НА КИБЕРОТБРАНАТА КЪМ АЛГОРИТМИТЕ: ПРАВНИ ГРАНИЦИ НА АВТОНОМНИЯ ОТГОВОР В БЪЛГАРИЯ

Резюме: *Статията изследва правните последствия от възможностите за автономен отговор в българската система за киберотбрана. Тя анализира правната рамка и я поставя в широкия контекст на стратегически документи на НАТО и ЕС. Статията определя и изследва правната жизненост на автономния киберотговор, подчертавайки как автоматизирани отбранителни действия отправят предизвикателство към съществуващите правни стандарти. Еволюцията на българската позиция спрямо киберотбраната е документирана с преход от първоначални отбранителни стратегии към синхронизиране с актуални директиви на ЕС и изисквания на НАТО. Дискусията разкрива, че българското законодателство не предлага специфично правно разрешение за автоматизирани контрамерки в случай на кибератака. Статията заключава, че докато в българското законодателство съществува ясна база за борба с киберпрестъпността и защитата на критична инфраструктура, в него има значителни предизвикателства по отношение на включването на автономни киберотговори. Статията отчита презумпцията, че разработката на всяка стратегия изисква съвместимост с международните ангажименти на страната.*
Ключови думи: *киберотбрана; автономен отговор; изкуствен интелект; правна рамка; законодателство*

гл. ас. д-р Владимир Бабанов
ORCID 0000-0001-8596-6493, SCOPUS ID: 60021493300
Югозападен университет „Неофит Рилски”
Благоевград, България
E-mail: v.babanov@law.swu.bg