CYFROWY PARALIŻ PAŃSTWA

Czy Policja wytrzyma starcie w wojnie hybrydowej nowej generacji?

Grafika wygenerowana z wykorzystaniem licencjonowanego programu Adobe Firefly.

Marcin Tęgos

Naczelnik Wydziału Cyberbezpieczeństwa Biura Łączności i Informatyki KGP
Przewodniczący Zespołu POL-CERT

W świecie, gdzie granica między pokojem a konfliktem uległa całkowitemu zatarciu, prawdziwe pole bitwy nie leży na polach czy w pasie przygranicznym, lecz w krzemowych obwodach naszych serwerów. Podczas gdy opinia publiczna patrzy na Policję przez pryzmat radiowozów i patroli, najważniejsza instytucja mająca za zadanie ochronę bezpieczeństwa i utrzymanie porządku publicznego walczy dziś na pierwszej linii frontu niewidzialnej wojny. Teza jest brutalnie prosta: jeśli zawiedzie cyberbezpieczeństwo infrastruktury Policji, całe państwo może doświadczyć cyfrowego paraliżu, zanim pierwszy funkcjonariusz zdąży wyciągnąć broń.

Przez lata popełnialiśmy błąd poznawczy. Myśleliśmy o cyberbezpieczeństwie w kategoriach „walki z przestępcami" – ścigania hakerów kradnących dane czy oszukujących emerytów. To myślenie jest anachroniczne i niebezpieczne. Dziś cyberbezpieczeństwo Policji to nie tylko kwestia łapania złodziei, to fundament bezpieczeństwa wewnętrznego państwa.

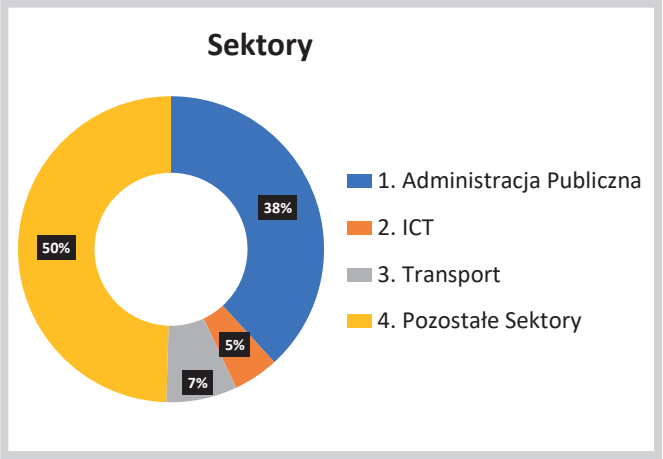
Spójrzmy na liczby, bo one nie kłamią i nie mają emocji. W roku 2025 Wydział Cyberbezpieczeństwa Biura Łączności i Informatyki Komendy Głównej Policji wraz z zespołem POL-CERT obsłużył ponad 17 tysięcy incydentów. To o ponad pięć tysięcy więcej niż rok wcześniej. To nie jest „wzrost statystyczny" – to potężna fala uderzeniowa, która każdego dnia rozbija się o mury naszej instytucji. I co najgorsze: ta fala nie słabnie, ona przybiera na sile, napędzana przez geopolityczne ambicje adwersarzy, dla których infrastruktura rządowa i policyjna jest celem priorytetowym.

Sektor publiczny w Polsce znajduje się pod bezprecedensową presją cyberataków. W 2024 r. cyberprzestępcy dokonywali średnio 2063 ataków miesięcznie na sektor publiczny oraz 2058 ataków na sektor wojskowo-rządowy[1]. W 2024 r. odnotowano wzrost liczby incydentów w sektorze publicznym o 58 procent w porównaniu do roku 2023[2].

Dane z pierwszej połowy 2025 r. wskazują na dalszą eskalację zagrożeń. W analizowanym okresie zgłoszono 485 tysięcy potencjalnych incydentów bezpieczeństwa, z czego potwierdzono 111 660 przypadków rzeczywistych naruszeń – wzrost o 23 procent. Szczególnie alarmujące są dane dotyczące ataków o poważnym charakterze, których liczba wzrosła o 57 procent, a naruszeń w sektorze publicznym o 58 procent[3].

Według raportu ENISA, polska administracja publiczna znalazła się w gronie pięciu państw najbardziej atakowanych w UE, z udziałem 15 procent incydentów w tej kategorii[4].

Wykres nr 1. Cele ataków cybernetycznych w stosunku do liczby zgłoszonych incydentów. (Zestawienie na podstawie danych Agencji Unii Europejskiej ds. Cyberbezpieczeństwa – ENISA 2024-2025 EU, dla sektorów określonych w dyrektywie NIS2[5]).



Wchodzimy w erę, w której grupy APT[6] nie szukają już tylko pieniędzy. Szukają chaosu. Szukają sposobu na wyłączenie systemów łączności, paraliż komunikacji kryzysowej i ośmieszenie instytucji państwowych. Co więcej, nadchodzi „cyfrowy darwinizm" – era wspierana przez sztuczną inteligencję (AI), gdzie automatyczne ataki będą generowane z prędkością, której ludzki operator nie jest w stanie się przeciwstawić. Standardowe procedury, które dziś wydają się solidne, jutro mogą stać się jedynie cyfrowym odpowiednikiem papierowych tarcz przeciwko pociskom rakietowym. W tym kontekście działania Biura Łączności i Informatyki KGP – choć wciąż będące zaledwie początkiem długiej drogi – jawią się jako niezbędna próba „podjęcia rękawicy". Nie możemy pozwolić sobie na reaktywność; musimy przejść do strategii proaktywnej. Reforma zarządzania, przebudowa struktury POL-CERT i dostosowanie do rygorystycznych wymogów nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa to nie są tylko biurokratyczne zabiegi. To budowa cyfrowego układu odpornościowego. Centralizacja zarządzania stacjami roboczymi oraz wprowadzenie twardej, sprzętowej autoryzacji (2FA[7]) to fundamenty, bez których każda próba obrony jest skazana na porażkę. Bez tego Policja pozostaje instytucją z „otwartymi drzwiami" w świecie, gdzie każdy atak jest zautomatyzowany i nieubłagany.

Musimy jednak zadać sobie pytanie: czy to wystarczy? Wyścig zbrojeń między państwową machiną a grupami hakerskimi wspieranymi przez obce mocarstwa to bieg, w którym stawką jest suwerenność informacyjna. Inwestycja w technologię to tylko połowa sukcesu. Drugą połową jest kapitał ludzki – szkolenie kadr, które będą potrafiły myśleć krok przed algorytmem przeciwnika.

Policja nie może być postrzegana jedynie jako instytucja reagująca na przestępstwa. Musi stać się twierdzą, której cyfrowe mury są równie szczelne, co fizyczne zapory. Jeśli nie zrozumiemy, że bezpieczeństwo infrastruktury IT Policji jest tożsame z bezpieczeństwem każdego obywatela, obudzimy się w państwie, które ma wszystkie paragrafy świata, ale nie posiada sprawnego systemu, by je wyegzekwować.

[1] ISBtech.pl. Serwis o tematyce technologicznej, *Ponad 4 000 ataków miesięcznie na polski sektor publiczny*, https://www.isbtech.pl/2025/05/ponad-4-000-atakow-miesiecznie-na-polski-sektor-publiczny/ [dostęp: 11.06.2026 r.].

[2] Z. Łochowska, *Statystyki cyberbezpieczeństwa: co mówią dane o wzroście zagrożeń w 2025 roku?*, Exorigo-Upos.pl, https://www.exorigo-upos.pl/blog/statystyki-cyberbezpieczenstwa-dane-z-2025-roku/ [dostęp: 11.06.2026 r.].

[3] J. Jaśkowiak, *Cyberzagrożenia w Polsce 2025: Najczęściej atakowana infrastruktura krytyczna*, Mikrokontroler.pl, 25.04.2025 r., https://mikrokontroler.pl/2025/04/25/cyberzagrozenia-w-polsce-2025-najczesciej-atakowana-infrastruktura-krytyczna/ [dostęp: 11.06.2026 r.].

[4] ENISA. European Union Agency For Cybersecurity, Enisa Threat Landscape 2025, październik 2025 r., s. 18,https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf [dostęp: 11.06.2026 r.].

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.U. L 333 z 27.12.2022, pp. 80–152.

[6] Grupy APT (*Advanced Persistent Threat* – zaawansowane trwałe zagrożenie) – grupy cyberprzestępców skupiające się na zaawansowanych, trwałych zagrożeniach. Są to zazwyczaj cyberprzestępcy z organizacji państwowych lub organizacji, które działają w imieniu państw. Koncentrują się one na ukierunkowanych i wyrafinowanych operacjach cybernetycznych, aby przeniknąć do systemów wysokiego szczebla (organizacji rządowych, korporacji) i pozostać w nich niewykrytymi przez dłuższy czas. Działają głównie w celu długoterminowego cyberszpiegostwa i kradzieży poufnych danych. Dysponują zaawansowanymi narzędziami, technikami, wiedzą i umiejętnościami. Źródło: ESET Online Help, ESET Glossary, https://help.eset.com/glossary/pl-PL/apt_group.html [dostęp: 11.06.2026 r.].

[7] Sprzętowa autoryzacja 2FA – jedna z najbezpieczniejszych form weryfikacji tożsamości polegająca na logowaniu się fizycznym kluczem – urządzeniem USB lub NFC, które generuje kryptograficzny podpis.

Summary

Digital paralysis of the state: can the Police withstand the new era of hybrid warfare?

The author, Head of the Cybersecurity Department at the Communications and Information Technology Bureau of the National Police Headquarters, outlines a fundamental shift in the way public security and public order are safeguarded. While the public often associates police work with patrol cars and officers on the streets, the Police are increasingly operating on the frontlines of cyberspace. The author argues that a failure to adequately protect police information and communication systems could lead to digital paralysis with consequences extending far beyond the Police itself. In 2025, the Cybersecurity Department of the National Police Headquarters and the POL-CERT team handled nearly 17,000 cybersecurity incidents – over 5,000 more than in the previous year. According to the author, this trend shows no sign of slowing down and is, in fact, becoming increasingly pronounced. Particular attention is paid to Advanced Persistent Threat (ATP) attacks aimed at creating chaos, disrupting communications, impairing crisis-management capabilities, and discrediting state institutions. The growing use of artificial intelligence is expected to further increase both the scale and sophistication of such threats. The article concludes that the Police must adopt a proactive approach strengthening cyber resilience. This will require organisational reform, the further development of the POL-CERT framework, compliance with the amended National Cybersecurity System Act, and continued investment in highly skilled cybersecurity professionals capable of staying ahead of increasingly sophisticated threats.

Tłumaczenie: Joanna Łaszyn