Wielu przypuszcza, że cyberataki nie mogą zabijać ludzi. To nieprawda

Cyberataków nie należy lekceważyć i traktować jako niewinnej zabawy młodych ludzi. To poważne przestępstwa, które mogą prowadzić również do śmierci.

- Grupa ekspertów ostrzega, że □□Korea Północna mogłaby wykorzystać techniki groźnych cyberataków.
- Cyberprzestępcy mogą na przykład przejąć kontrolę nad oczyszczalnią wody i zmienić mieszankę chemiczną, aby była toksyczna…
- …albo przeniknąć do systemów komputerowych elektrowni jądrowej, powodując poważne awarie.

Koreański dziennikarz Jung Min-ho pisze:

> *Jednym z najbardziej niedocenianych zagrożeń bezpieczeństwa pochodzących z Korei Północnej są jej możliwości cyberataków. Wielu przypuszcza, że □□hakerzy nie mogą zabijać ludzi. Ale mogą.*

Cyberprzestępcy mogą przejąć kontrolę nad oczyszczalnią wody i zmienić mieszankę chemiczną, aby była toksyczna, lub mogą przeniknąć do systemów komputerowych elektrowni jądrowej, powodując poważne awarie. W ostatnich latach w wielu częściach świata podejmowano próby takich cyberataków, niektóre z nich zakończyły się pośrednio śmiercią lub obrażeniami.

Grupa ekspertów ostrzega, że □□Korea Północna mogłaby wykorzystać takie techniki, gdyby wybuchła wojna na Półwyspie Koreańskim, w raporcie RAND Corporation zatytułowanym "Charakterystyka zagrożeń związanych z północnokoreańską bronią chemiczną i biologiczną, impulsem elektromagnetycznym i zagrożeniami cybernetycznymi".

Choi Kang, prezes Asan Institute for Policy Studies i jeden ze współautorów wspólnego raportu napisanego z think tankiem RAND Corporation, powiedział na konferencji prasowej w instytucie w Seulu we wtorek.

> *Infrastruktura w Korei Południowej wydaje się być bardzo podatna na cyberataki Północy. Widzieliśmy kilka przypadków w systemach bankowych… Ale co z inną infrastrukturą, taką jak zaopatrzenie w wodę lub elektryczność? To spowodowałoby chaos.*

Możliwe scenariusze

Jednym z możliwych scenariuszy może być wykolejenie pociągów załadowanych śmiercionośnymi chemikaliami. Inne możliwe cele obejmują tamy, szpitale, lotniska i sieci energetyczne, których wiele systemów komputerowych zostało już wcześniej przeniknięty przez Koreę Północną.

Raport mówi, że domniemane rozmieszczenie wirusa Stuxnet przez Stany Zjednoczone i Izrael w celu uszkodzenia irańskich wirówek do wzbogacania nuklearnego oraz rosyjski program złośliwego oprogramowania towarzyszący inwazji na Ukrainę w tym roku mogą służyć jako przykłady do naśladowania i rozwijania przez Koreę Północną.

Źródło