Exploding Pagers and the Birth of State Cyberterrorism

Fabio Massacci | University of Trento and Vrije Universiteit Amsterdam

There are symbols that historians use to exemplify nonreturning points in the way technology changes warfare, and the Israeli exploding pagers mark the birth of state cyberterrorism.

The explosives-laced, cyberactivated pagers that Israel unleashed on Lebanon will become a symbol of technological and political change, as significant as the iron stirrups of the Mongols of Ghengis Khan, which allowed nomads to transform into an invincible horde; the longbows of the archers of England, which made it possible to defeat the mounted knights of the French cavalry at Azincourt; or the arquebuses of the Spanish musketeers, which massacred an overwhelming number of Aztecs during Tenochtitlan's siege.

These symbols rarely have a good reputation. In a prescient article that appeared in this magazine,[1] we discussed when a lethal autonomous cyberweapon would be a lawful or unlawful one. There is a thin but not invisible boundary between state war and state terrorism.

First, let's recap how the attack was actually organized. Israeli intelligence, operating through Hungarian shell companies (for example, B.A.C. Consulting)[2] working on a license by a Taiwanese company (Gold Apollo), "enhanced" pagers with batteries in which a small amount of PETN, an explosive that is difficult to detect, was laced. A special encrypted message would activate the detonation, allegedly if the pager holder read the encrypted message, or through a second activating message.[3] From the description of the news,[4] it is clear that the sending of the second messages was the actual cause of the overwhelming majority of the detonations (involving people driving motorbikes, medical staff, or even children carrying the pagers to their parents). The few videos available on the event clearly show that the detonation happened in the bag.[3] That Israel was behind the attack has been actually recognized officially today[5] (at the time of this writing).

From the perspective of *supply chain security*, this is an interesting scenario that modern research on supply chain security has not considered in either the physical[6] or the digital domain.[7] If one considers the use of blockchain technology to actually trace back and authenticate in a hardware bill of material the pagers as Internet of Things objects,[8] the explosive pagers would have obtained a bill of health as they have been appropriately licensed and produced through the appropriate chain of parties.

Indeed, the major assumption in all supply chain research is that the authentic actors are essentially trustworthy, and we must only avoid a situation in which some of the steps are inadvertently subverted. Israel showed that the equation authentic actors = good actors is unwarranted.

The world is much closer to the one we described in the "'Free' as in Freedom to Protest?" piece,[9] in which the threats are very people who are supplying us the software or the hardware and who can unleash indiscriminate attacks to foster their political agendas. Obviously, formatting all computers that have a Russian keyboard to support Ukraine is not at the same level as

Digital Object Identifier 10.1109/MSEC.2024.3500114
Date of current version: 20 January 2025

blowing up all pagers because they have been procured through the same channel that serves Hamas.

Yet, one of the major ethical issues in the protestware attacks has been precisely the untargeted nature of the attack.

Targeted assassination of individual enemies is considered part of the "dirty job" of intelligence services,[10] and while the United States has mixed successes,[11] Israel actually successfully staged one such individual attack when it assassinated Yahya Ayyash, one of the leaders of Hamas suicide bombers.[12]

The Ayyash attack is very similar to the pagers attack with a *small technical difference* that makes a *huge political and legal difference*. The Israeli intelligence contacted (or were contacted by) a member of the Ayyash household and gave him a cellular phone that allowed them to track and listen to calls. The phone was also laced with explosives. At some point when Ayyash used the phone to make a call, the call was intercepted by an Israeli plane, which, recognizing Ayyash, detonated the explosive and killed him.

So what is the technical difference? This is clear to any cyberspecialist: the Ayyash attack was a *targeted* attack; the Lebanon pagers attack was *untargeted*. More than 5,000 of such pagers were imported,[3] and it is actually surprising that only 3,000 people were actually injured.

It can be argued that the owners of the pagers could have been mostly Hamas militants, but this is the same as arguing that if an Internet service provider (ISP) mostly hosts malware, then all clients of the ISP are malicious and could be legitimately victimized by a retaliatory malware unleashed on the ISP. This is indeed one of the least convincing cases illustrating the Association for Computing Machinery Code of Ethics.[13] Unsurprisingly, the case no longer has a public author willing to stand behind this analysis (somewhere on my hard disk I have the printed page with the name of the author, but I can't find it).

Israel is, jointly with USA, Russia, China, and several other European countries, a signatory party to Amended Protocol II of the Convention on Certain Conventional Weapons (CCW),[14] which addresses *booby traps*. The full title of the convention is very long but ends with the telling phrase "to have indiscriminate effects."

So, for the uninitiated, what is a booby trap? Article 2 of the CCW spells it for us [my emphasis]: "Booby-trap" means ***any device*** or material which is designed, constructed or ***adapted to kill*** or injure, and which functions ***unexpectedly*** when a person disturbs or approaches ***an apparently harmless object*** or performs ***an apparently safe act***." Article 7 of the protocol explicitly prohibits the use of such booby traps.

In our article on lawful cyberweapons,[1] we identified few key aspects that define unlawful weapons from a technical and target perspective (Table 1 and Table 3):[1]

- The impossibility of recognizing and deactivating the cyberweapons after the conflict is over is against the principle of proportionality and unnecessary suffering (as the pagers would still look like pagers, but the batteries laced with explosives would still be laced with explosives).
- Indiscriminate payload unleashing is against the principle of proportionality as the precise target should be defined offline (this is indeed what differentiated the Ayyash attack from the Lebanon attack).

One can appreciate the futile attempts by Israeli legal scholars[15] to invent justifications on the *jus ad*

Digital Object Identifier 10.1109/MSEC.2024.3518993

bellum (the right to war) for such deployment, but claiming that pagers are military objects and therefore all holders of a pager are military targets is frankly too significant a stretch.

As the Air Commodore (retired) Bill Boothby, the coauthor of the *NATO Tallinn Manual on the International Law Applicable to Cyber Warfare*, put it, "The pager is being adapted to convert it into a booby-trap of the sort addressed by Article 7(2) of Amended Protocol II and on that basis it would appear [...] to be an unlawful weapon."[16]

This year, Israel crossed the thin (but not invisible) line, and state cyberterrorism was born. ■

Acknowledgement

This work is partly supported by the European Union under grant 101120393 (Sec4AI4Sec) and the Dutch Research Council (NWO) under grant NWA.1215.18.006 (HEWSTI). The opinions expressed in this article are the author's and should not be attributed to either funder or IEEE.

References

1. F. Massacci and S. Vidor, "Building principles for lawful cyber lethal autonomous weapons," *IEEE Security Privacy*, vol. 20, no. 2, pp. 101–106, Mar./Apr. 2022, doi: 10.1109/MSEC.2022.3143269.
2. M. Untersinger. "Companies behind exploding pagers targeting Hezbollah members difficult to trace," *Le Monde*, Sep. 24, 2024. [Online]. Available: https://www.lemonde.fr/en/pixels/article/2024/09/24/companies-behind-exploding-pagers-targeting-hezbollah-members-difficult-to-trace_6727076_13.html
3. M. Murphy and J. Tidy, "What we know about the Hezbollah device explosions," *BBC News*, Sep. 20, 2024. [Online]. Available: https://www.bbc.com/news/articles/cz04m913m49o
4. S. Frenkel, R. Bergman, and H. Saad, "How Israel built a modern-day Trojan horse: Exploding pagers," *The New York Times*, Sep. 18, 2024. [Online]. Available: https://www.nytimes.com/2024/09/18/world/middleeast/israel-exploding-pagers-hezbollah.html
5. "Netanyahu says he 'greenlighted' Lebanon pager attacks," *Le Monde*, Nov. 10, 2024. Available: https://www.lemonde.fr/en/international/article/2024/11/10/netanyahu-says-he-greenlighted-lebanon-pager-attacks_6732328_4.html
6. G. Lu, X. Koufteros, and L. Lucianetti, "Supply chain security: A classification of practices and an empirical study of differential effects and complementarity," *IEEE Trans. Eng. Manag.*, vol. 64, no. 2, pp. 234–248, May 2017, doi: 10.1109/TEM.2017.2652382.
7. R. J. Ellison, J. B. Goodenough, C. B. Weinstock, and C. Woody, "Evaluating and mitigating software supply chain security risks," Software Eng. Inst., Tech. Rep. CMU/SEI-2010-TN-016, 2010.
8. V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, "A survey on supply chain security: Application areas, security threats, and solution architectures," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6222–6246, Apr. 2021, doi: 10.1109/JIOT.2020.3025775.
9. F. Massacci et al., "Free" as in freedom to protest?" *IEEE Security Privacy*, vol. 20, no. 5, pp. 16–21, Sep./Oct. 2022, doi: 10.1109/MSEC.2022.3185845.
10. W. Thomas, "Norms and security: The case of international assassination," *Int. Secur.*, vol. 25, no. 1, pp. 105–133, 2000, doi: 10.1162/016228800560408.
11. D. W. Belin. "Summary of facts. Investigations on CIA's involvement in plans to assassinate foreign leaders." Gerald R. Ford Presidential Library. Accessed: Nov. 10, 2024. [Online]. Available: https://www.fordlibrarymuseum.gov/sites/default/files/pdf_documents/library/document/0005/7324009.pdf
12. "Yahya Ayyash." Wikipedia. Accessed: Nov. 10, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Yahya_Ayyash
13. "Case: Malware disruption." ACM. Accessed: Nov. 10, 2024. [Online]. Available: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/
14. "Convention on prohibitions or restrictions on the use of certain conventional weapons which may be deemed to be excessively injurious or to have indiscriminate effects." ICRC. Accessed: Nov. 10, 2024. [Online]. Available: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0811.pdf
15. A. Cohen and Y. Shany, "Well, it depends:explosive pagers attack revisited," in *Articles of War*. Westpoint, NY, USA: Lieber Institute, United States Military Academy, Oct. 11, 2024.
16. W. H. Boothby, "Exploding pagers and the law," in *Articles of War*. Westpoint, NY, USA: Lieber Institute, United States Military Academy, Sep. 18, 2024.

Fabio Massacci is a professor at the University of Trento, 38123 Trento, Italy, and Vrije Universiteit Amsterdam, 1081 HV Amsterdam, The Netherlands. His research interests include empirical methods for the cybersecurity of sociotechnical systems. Massacci received a Ph.D. in computing from the Sapienza University of Rome. He leads the Horizon 2020 AssureMOSS project and the Horizon Europe Sec4AI4Sec and the Dutch NWO project HEWSTI. For his work on security and trust in sociotechnical systems, he received the Ten Year Most Influential Paper Award at the 2015 IEEE International Requirements Engineering Conference. He is named co-author of CVSS v4.0. He is a Member of IEEE. Contact him at fabio.massacci@ieee.org.