Cyber mercenaries: An old business model, a modern threat

Cybersecurity Tech Accord principles limiting offensive operations in cyberspace

Cyberspace is increasingly seen as an area of conflict and strategic contestation between states. However, developing and sustaining offensive and intrusive cyber capabilities is usually expensive, time consuming, and labor intensive; requiring skills most countries do not have or cannot maintain over time. This has led to the emergence of cyber mercenaries, which includes private sector actors willing to develop and provide these capabilities to countries and enterprises for a fee. While leveraging cyber mercenaries may appear appealing to countries looking to deploy such methods, the unmitigated expansion of this marketplace threatens to severely destabilize the broader online environment in the long run.

There are numerous terms used to describe this growing sector, including "cyber mercenaries," "intrusion as a service," "surveillance-for-hire" or simply "private sector offensive actors." For the purposes of this document, the term "cyber mercenaries" is defined as companies - or occasionally individuals - dedicated to developing, selling, and supporting offensive cyber capabilities which enable their clients - often governments - to access the networks, computers, phones, or internet-connected devices in ways that violate human rights and undermine democratic principles.

Building on the Cybersecurity Tech Accord's principal commitments, Tech Accord signatories have led the development of a set of industry principles to tackle the rising threat posed by cyber mercenaries. These principles are not intended to affect compliance with existing legal obligations and any implementation by industry partners will be in line with their own policies and processes, as applicable.

The implementation of these industry principles will also be informed by governmental processes that restrict the export of certain sensitive technologies and components to cyber mercenaries (such as the US export controls Entity List, and similar European Union (EU) and Organisation for Economic Co-operation and Development (OECD) member country designations).

Cybersecurity Tech Accord signatories and other industry partners support the following principles that reflect good practices:

1. Take steps to counter cyber mercenaries' use of products and services to harm people

- Conduct human rights due diligence in line with the United Nations Guiding Principles on Business and Human Rights[1] to identify risks and mitigations related to possible misuse of products and services by cyber mercenaries.
- Issue cease and desist letters and/ or take other lawful action against cyber mercenaries, as appropriate.
- Share information with each other, industry peers, as well as with researchers and civil society partners on cyber mercenary attacks, as well as identified trends, and potential mitigations, as appropriate.

[1] Guidingprinciplesbusinesshr_en.pdf (ohchr.org)

2. Identify ways to actively counter the cyber mercenary market

- Ensure compliance with legal restrictions targeting the cyber mercenary market, including the US Entity List or other similar designation processes.[2]
- Promote wider compliance with international human rights standards and laws and increase awareness on how to prevent products and services from being misused to commit human rights abuses informed by existing governmental guidance (e.g., the U.S. Department of State Guidance on Implementing the "UN Guiding Principles"[3]).
- Advocate for the development, adoption, and use of coordinated governance frameworks, policy guidelines, and regulation to effectively limit export and import of, and investments in information technology products and services used and developed by cyber mercenaries.

3. Invest in cybersecurity awareness of customers, users and the general public

- Increase public awareness and education on the issue of cyber mercenaries, as well as possible remedies by providing customers and users with appropriate resources, guidance, and tools to ensure that they can protect themselves online and build their overall cyber resilience.
- Help customers and users improve cybersecurity practices and resilience in partnership with civil society organizations committed to building capacity, such as those supporting particularly targeted groups.

4. Protect customers and users by maintaining the integrity and security of products and services

- Develop and deploy tools to detect patterns of behavior associated with malicious activity by cyber mercenaries to increase protections of products and services.
- Maintain and promote strong encryption for products and services as feasible and not knowingly weaken the security of customers and users to facilitate electronic surveillance or access by cyber mercenaries.
- Notify customers and users whose accounts are reasonably believed to have been targeted by cyber mercenaries where feasible and as appropriate.

5. Develop processes for handling valid legal requests for information

- Establish and maintain processes to ensure government agencies and law enforcement authorities can submit lawful requests for information in accordance with applicable laws and international standards, including their human rights obligations.

---

[2] Entity List (doc.gov)
[3] Due Diligence Guidance - United States Department of State

- Establish and maintain processes to safeguard such processes from attempted exploitation by cyber mercenaries and other bad actors.
- Increase transparency of the law enforcement requests process, such as by making the number of requests companies receive public.

Endorsing companies:

1. Cisco (principal co-author)
2. Meta (principal co-author)
3. Microsoft (principal co-author)
4. Trend Micro (principal co-author)
5. 10Pearls
6. Apple
7. Archive360
8. AvePoint Inc
9. Balasys IT
10. Big Cloud
11. Bitdefender
12. Contrast Security
13. DXC
14. ESET
15. European Business Reliance Centre (EBRC)
16. G DATA
17. GitHub
18. Globant
19. Google
20. Greenlight Information Services
21. ImmuniWeb
22. LaSalle Consulting Partners, Inc.
23. Lenovo
24. Madison Computer Works
25. Northwave Cyber Security
26. onShore Security
27. Pax8
28. Professional Options LLC
29. ReSecurity
30. SafePC Solutions
31. Silent Breach
32. Summit V
33. Telefonica
34. US Licensing LLC
35. US Medical IT
36. Validy Net Inc.
37. WCA Technologies
38. Wipfli LLP
39. WISeKey
40. WithSecure