ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 10/25 (October) – Special Edition Op-Ed

From Privacy to Power: Why Defence Must Confront the Weaponisation of Data

By Benjamin Ang

DATA IS A DEFENCE PROBLEM

1. A few months before time of writing, a group of senior U.S. defence officials inadvertently leaked sensitive military operational plans about military strikes against the Houthis in Yemen while discussing them in a Signal group chat. The leak did not arise from any breach of the app's end-to-end encryption, but from someone accidentally adding an unauthorized individual, a journalist, to the conversation.

2. This happened just one year after Russian media leaked an audio recording of sensitive military discussions, about the war in Ukraine, from a confidential Webex video call between senior German military officials. This call had reportedly been intercepted when one of the callers had dialled into Webex using unsecured hotel Wi-Fi.

3. A European news site reported a few months later that they were still able to access online meeting rooms of 6,000 Webex meetings attributed to 248,000 German soldiers because of weak online security design.

4. Data security leaks still plague military personnel using civilian technology, almost a decade after analysts discovered leaks from the Strava fitness tracking app. Strava had published a data visualisation map that not only displayed the jogging routes of all its users, but in the process inadvertently revealed the location and perimeters of secret military bases, and even the routes taken by military personnel on exercise in conflict zones.

5. This app has been so effective in leaking military data that it has spawned its own series of "Stravaleaks" which include the patrol schedule of France's atomic-armed submarines (because of crew movement), and movements of secret service agents assigned to protect U.S. President Donald Trump and former U.S. President Joe Biden.

6. Such data leaks can be quickly weaponised during conflict. A Russian volunteer in eastern Ukraine posted pictures and videos of himself and members of his Brigade on VKontakte (Russia's equivalent of Facebook) with location tracking activated, which enabled Ukrainian forces to find them and destroy their location.

7. With all these examples, it would be a strategic blind spot to imagine that personal data security is only a concern for civilian privacy and personal data protection. Data is no longer just a privacy issue but a battlefield asset. Our soldiers, civilians supporting troops, defence contractors, and their devices, all leave digital footprints that can be weaponised as a vector for surveillance, disruption, and influence. These footprints include social media activity, location history, and even health metrics. Thanks to widespread advances in artificial intelligence (AI), even a middle power adversary can aggregate and analyse these data points to gather intelligence. The wave of digital transformation that is bringing economic prosperity to small states can also enable them to weaponise data for military use.

HOW DATA CAN BE WEAPONISED

8. Some of the ways these analysed data can be weaponised include (1) Surveillance and profiling; (2) Guiding deception and blackmail operations; (3) Tailoring disinformation and influence operations; and (4) Situational awareness and operations.

9. Specifically, **surveillance and profiling** of locations, activities, and identities of military personnel has been well exploited as shown in the earlier examples. Additionally, data on personal connections, affiliations, and personal interests of military personnel can be used for targeting them.

10. In addition, adversaries can use data for **guiding deception and blackmail operations** that target individual military personnel with tailored falsehoods or exploiting their private vices. Adversaries can also identify individuals vulnerable to blackmail, coercion, or targeted manipulation because of their financial pressures, personal grievances, or hidden habits, with huge potential for espionage and sabotage.

11. Further, adversaries can use data for **tailoring disinformation and influence operations** with differentiated narratives that fit different demographics of the defence force. The use of Dark Posts is a common marketing method on social media, where posts do not appear to the public but only in the feeds of users that are specifically targeted for each specific message. Since some Southeast Asian states have defence forces that are multiracial, multicultural, or multireligious, adversaries can target falsehoods or biased posts to exploit social faultlines, to sow discord and distrust.

12. One apparently successful wartime use of **situational awareness and operations** from weaponised data is Ukraine's Delta system, which is a software system designed to gather data from drones, satellites, cameras, and sensors, then analyse it, provide comprehensive situational awareness, and support battlefield decision-making, including where and how to strike Russian targets.

CHALLENGES FOR THE DEFENCE SECTOR

13. Defence officials who recognise the threat from the weaponisation of data face several challenges. Firstly, such operations may take place as preparatory acts below the threshold of armed conflict, so they are difficult to detect and respond to. Within this grey zone, adversaries may also target the civilian families of military personnel.

14. Secondly, adversaries can easily harvest data from civilian platforms, either by breaching their security, or by outright purchase from data brokers. Several countries have also passed laws that empower them to compel companies to hand over or give access to data for national security reasons (which can be invoked in times of conflict), including the U.K., U.S., China, India, Australia, Russia, and Saudi Arabia.

15. Thirdly, many nations depend on digital infrastructure and platforms that are owned by foreign companies. This exposes both civilians and military personnel to surveillance, coercion, or sabotage. Sabotage from technology companies can have a huge impact on military operations or even survival, as seen from the allegations that U.S.-based Starlink cut off satellite services during key Ukrainian military operations, resulting in blackouts of communications, surveillance, and targeting, that caused at least one attack to fail.

16. The latter two challenges arise because the private sector holds most data which can be weaponised, but there are inadequate frameworks for the defence sector to engage the private sector for the protection of this data or response to its weaponisation, especially in Southeast Asia. The Atlantic Council's "Sixth Domain" report argues that the private sector must now be considered a full-

fledged domain of warfare. The report recommends inter alia that government should develop frameworks for effective engagement with and coordination of the role of the private sector in wartime.

STRATEGIC RESPONSES

17. To confront the weaponisation of data, defence agencies must move beyond reactive compliance and treat data as a strategic key battlefield asset.

18. Defence agencies can start with surveying the data terrain by conducting data exposure simulations across military and civilian platforms, to discover what digital footprints are left by the apps and devices used by personnel. This knowledge can then be used to develop a data strategy for the defence sector. This strategy should include policies on the use of civilian technology by military personnel. It should be supported by OPSEC training, including social media hygiene, care of location settings, and app permissions. Forces should also train personnel so they are aware that their data can be used to manipulate morale, create discord, or be used for blackmail.

19. This will be challenging for states that need capacity building in these areas. For Southeast Asian countries, one solution may be to engage regional organisations like the ADMM Cybersecurity and Information Centre of Excellence (ACICE) who can partner with cross-sectoral experts from the private sector, academia, and civil society. This partnership should also build public awareness across the society, not just within defence, because military personnel are inevitably connected to their civilian family and friends.

20. The weaponisation of data is not a future threat, but an active battlespace that defence agencies must urgently navigate. As adversaries exploit digital footprints for surveillance, manipulation, and disruption, the defence sector must evolve strategies of treating data as terrain, building cross-sectoral partnerships, and embedding data hygiene into every layer of operations. Southeast Asian states should invest in capacity building and regional coordination to safeguard their forces and societies. The ability to secure and wield data may determine operational success and national survival, so the time to adapt is now, before the next breach isn't accidental, but adversarial.

**The views expressed in this Cyber Digest are that of Benjamin Ang, a member of ACICE's Experts Panel. Benjamin is Head of the Centre of Excellence for National Security, Future Issues and Technology, and Digital Impact Research, at the S Rajaratnam School of International Studies, Nanyang Technological University. He leads the teams that research security strategy and policy in cybersecurity, cyber conflict, cybercrime, information operations, foreign*

interference and hybrid warfare, polarisation and social resilience, and emerging technologies including AI, quantum, space, and biotechnology.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • • •

REFERENCES

1. Four lingering questions about Trump officials' Signal chat – BBC News
https://www.bbc.com/news/articles/c5y41xdrxnyo

2. Ukraine war: German call leak due to individual error, minister says – BBC News
https://www.bbc.com/news/world-europe-68467333

3. Over 6,000 German army meetings, some classified, accessible to anyone online – Le Monde
https://www.lemonde.fr/en/international/article/2024/05/04/over-6-000-german-army-meetings-some-classified-accessible-online-to-anyone_6670440_4.html#

4. Fitness tracking app Strava gives away location of secret US army bases – The Guardian
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

5. StravaLeaks: Dates of French nuclear submarine patrols revealed by careless crew members – Le Monde
https://www.lemonde.fr/en/videos/article/2025/01/13/stravaleaks-dates-of-french-nuclear-submarine-patrols-revealed-by-careless-crew-members_6737005_108.html

6. Strava app flaw revealed runs of Israeli officials at secret bases – BBC News
https://www.bbc.com/news/world-middle-east-61879383

7. Russian soldier gave away his position with geotagged social media posts – Task & Purpose
https://taskandpurpose.com/news/russian-military-opsec-failure-ukraine/

8. Biden and Trump put in danger by Secret Service agents: Watch the second episode of StravaLeaks – Le Monde
https://www.lemonde.fr/en/united-states/article/2024/10/28/biden-and-trump-put-in-danger-by-secret-service-agents-watch-the-second-episode-of-stravaleaks_6730825_133.html

9. U.S. Charges Chinese Military Officers in 2017 Equifax Hacking – The New York Times
https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html

10. Creating Facebook Unpublished/Dark Posts – Social Media Management
https://social-media-management-help.brandwatch.com/hc/en-us/articles/4491410571293-Creating-Facebook-Unpublished-Dark-Posts

11. Does Ukraine Already Have Functional CJADC2 Technology? – Center for Strategic & International Studies
https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology

12. Data Brokers: A Weak Link in National Security – S. Rajaratnam School of International Studies
https://rsis.edu.sg/staff-publication/data-brokers-a-weak-link-in-national-security/

13. Data Privacy Legal Trends 2025 – Clifford Chance
https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2025/02/data-privacy-legal-trends-2025.pdf

14. Musk ordered shutdown of Starlink satellite service as Ukraine retook territory from Russia – Reuters
https://www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/

15. The sixth domain: The role of the private sector in warfare – Atlantic Council
https://www.atlanticcouncil.org/in-depth-research-reports/report/the-sixth-domain-the-role-of-the-private-sector-in-warfare/