CyberCX Blog

Hamas-Israel conflict: Impacts for Australian and New Zealand organisations

Intelligence Update

CyberCX | Intelligence Update
Hamas-Israel conflict
Impacts for Australian and New Zealand organisations

Published by Cyber Intelligence 10 October 2023

On 8 October 2023, the Israeli Government formally declared war against Palestinian militant group Hamas, in response to a surprise attack by Hamas that killed over 700 people. This

Key Points

- We assess with moderate confidence that the Hamas-Israel conflict has **increased the likelihood** that ideologically-motivated actors will target AUNZ organisations with distributed denial of service (DDoS) attacks in the next month.
    - At least 30 groups ideologically aligned with Russia, Ukraine, India, Pakistan and Bangladesh have pivoted their social media channels and capability to the conflict.
    - It is **likely** that pro-Russia groups already known to target AUNZ will use the conflict and political responses to it—including physical protests in Australia—as a pretext to increase their campaigns in AUNZ.[1]
    - There is a **real chance** that other ideologically-motivated groups will target AUNZ organisations in direct response to the AUNZ governments' condemnation of Hamas in the next month.
    - While DDoS attacks are generally low impact, we have observed suspected Russian state-linked hacktivists using more sophisticated DDoS capabilities in 2023. It is also plausible that hacktivists will use website defacements or other disruptive tactics in AUNZ.
- We assess that AUNZ organisations face heightened risk of DDoS attacks associated with the conflict if they:
    - Operate in the financial services, energy and utilities, government, higher education, healthcare, media or airport sectors.
    - Have a presence in, or partnerships with, Israel or the surrounding region.
    - Are associated with political responses to the conflict, such as think tanks and universities, or corporations whose leaders or employees take a public stance.

Background

strikes. The timing of Hamas' surprise attack is significant, landing on the end of the Jewish festival of Sukkot and the 50th anniversary of the 1973 Yom Kippur war on the secular calendar.

  - The attacks killed civilians, including 260 at a music festival in southern Israel. The reported death toll on both sides is over 1,500 at the time of writing.[1]
  - On 8 October, Israel retaliated with large scale airstrikes against housing blocks, a mosque, tunnels and homes of Hamas officials in Gaza, killing over 400 people.[2]

- Israeli-Palestinian conflict is a longstanding, volatile flashpoint in the Middle East, impacting several regions globally. We assess the recent escalation into war will **almost certainly** impact the geopolitical balance in the Middle East and have flow-on impacts globally.
  - Demonstrators in at least Turkey, Iraq, Iran, Syria, Lebanon and Yemen have publicly shown support for Hamas and Palestinians.[3] We judge that flow-on effects from the conflict, including political unrest and violence, could encourage other Middle Eastern countries to align based on positions regarding the conflict.
  - The escalation will **almost certainly** inflame Iran-Israel and Iran-US tensions.
- Israeli-Palestinian conflict is also a lightning rod for global protest movements and, in some cases, political unrest and violence across Australia, Europe, Asia, and the US.
  - On 9 October, pro-Palestine demonstrators rallied in Sydney, celebrating Hamas' actions as "resistance" to Israeli occupation.[4] In response to the Australian Government lighting the Sydney Opera House with the Israeli flag, demonstrators threw flares outside the Sydney Opera House and chanted anti-Israel and anti-Jewish slurs. NSW Police warned Sydney's Jewish community to avoid the Sydney Opera House after green-lighting the pro-Palestinian demonstration.[5]
  - Globally, several governments, including France, Canada, Germany and the UK

- Like the Russia-Ukraine war [6], the Hamas-Israel war has mobilised significant hacktivist activity. In the two days following Israel's declaration of war:
    - At least 30 different groups have emerged in support for Israel or Hamas, with the overwhelming majority conducting attacks in support for Hamas (see Figure 1).[7]
    - At least one hacktivist operation "OpsRise" appears focused primarily on Israeli targets. Several hacktivist groups are using the longstanding "OpIsrael" to mobilise cyber attacks against Israeli targets.[8]
    - At least one hacktivist operation "OpAlliesOfIsrael" is primarily focused on Ukraine and governments that have condemned the attacks by Hamas.

    - Pro-Russia group, Anonymous Sudan, conducting DDoS attacks against the Jerusalem Post.
    - Hacktivist group, Indian Cyber Force, targeting Hamas' official portal.

Implications for AUNZ organisations

Increase of existing targeting of AUNZ by pro-Russia groups

- We assess it is **likely** that pro-Russia hacktivist groups known to target AUNZ will use these developments to increase the profile of their campaigns, either by revictimising organisations they have previously targeted or by widening their targeting lens.
    - The Russia-Ukraine war has demonstrated that AUNZ organisations are not out of sight or out of mind for pro-Russia hacktivists. The AUNZ governments' diplomatic support for Ukraine has driven pro-Russia hacktivist targeting of the government, media, healthcare, aviation and community sectors in **both countries.**
    - Protest activity in Australia may serve as a pretext to increase their campaigns in AUNZ.
- Several pro-Russia hacktivist groups have mobilised in response to the Hamas-Israel war, including **Killnet**, **Usersec**, **NoName057(16)** and **Anonymous Sudan**. At least two of these groups have targeted AUNZ, and one has previously used unrelated ideologically-motivated campaigns in Australia to pivot on to their own campaign activity.
    - In March and April, Anonymous Sudan joined a hacktivist campaign against Australia, dubbed "opAustralia". While we have moderate confidence opAustralia had authentic religious motivations,[9] a CyberCX Intelligence investigation revealed that Anonymous Sudan is unlikely to be an authentic hacktivist actor, based on its routine use of paid infrastructure and other tradecraft

attack most likely to impact AUNZ organisations, followed by website defacement and hack-and-leak attacks.

- Based on observed ideologically-motivated targeting connected to the Hamas-Israel conflict, along with pro-Russia group targeting we have observed in the last 12 months, we assess that AUNZ organisations face heightened risk if they:
    - Operate critical infrastructure, particularly financial services, energy and utilities, government, higher education, healthcare, media and airports.
    - Have a presence in, or partnerships with, Israel or the surrounding regions.
    - Are associated with political responses to the conflict, such as think tanks and universities, or corporations whose leaders or employees take a public stance.

New targeting of AUNZ by ideologically-motivated groups

- We assess there is a **real chance** that AUNZ organisations will be targeted by ideologically-motivated actors in direct response to AUNZ's condemnation of Hamas in the next month.
- We judge that other regions will be of higher strategic priority than AUNZ in the near term, but it is plausible that AUNZ organisations could be targeted.
    - The AUNZ governments, respectively, have condemned Hamas' actions and upheld Israel's right to defend itself. The Palestinian Authority's representative in Canberra described Australia's comments as "disappointing and regrettable".[10] AUNZ do not recognise Palestine.[11]

The spectre of destructive nation-state cyber attacks

- Based on available evidence, we assess there is a remote chance that AUNZ organisations will be affected by destructive attacks associated with this conflict, but this could change rapidly.

theatre of conflict.

  - While we do not currently have evidence to indicate these attacks are occurring at heightened scale or frequency, we note that Israel and Iran are known to conduct disruptive and destructive cyber attacks in response to diplomatic breakdowns.
  - Iran, a financial and political backer of Hamas, has the capability and intent to launch destructive cyber attacks against Israeli critical infrastructure. Further, pro-Iran ideologically-motivated actors have demonstrated intent and capability to target operational technology (OT) in the Middle East, with potential for significant physical impacts.
  - Iran has previously launched destructive cyber attacks against private sector organisations in the US in reprisal for US actions in the Middle East. Iran has also targeted other countries, including Albania, signalling their attacks were also aimed at Israel.[12]

[1] https://www.cbsnews.com/news/israel-hamas-war-death-toll-gaza-strip-palestinians-israelis-latest-news-day-3/

[2] https://www.reuters.com/world/middle-east/israeli-forces-clash-with-hamas-gunmen-after-hundreds-killed-2023-10-08/

[3] https://www.euronews.com/2023/10/08/israel-gaza-the-global-impact-of-the-escalating-conflict

[4] https://www.abc.net.au/news/2023-10-09/nsw-palestinian-rally-lakemba-sydney-israel-wong/102950238

[5] https://www.theaustralian.com.au/nation/police-to-jews-stay-away-from-sydney-opera-house-protest/news-story/29fd92eed36f6271f7f527645962c793

[6] https://cybercx.com.au/blog/how-russia-ukraine-conflict-is-reshaping-cyber-crime/

[7] Based on CyberCX Intelligence analysis of Telegram engagement.

[8] OpIsrael is an annual anti-Israel hacktivist campaign that launches coordinated DDoS attacks against Israeli

[10] www.smh.com.au%2Fpolitics%2Ffederal%2Faustralia-s-response-to-hamas-attacks-disappointing-says-palestinian-authority-20231008-p5eald.html

[11] https://www.dfat.gov.au/geo/occupied-palestinian-territories#:~:text=Political%20information,security%2C%20within%20internationally%20recognised%20borders.

[12] https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/05/Iran-turning-to-cyber-enabled-influence-operations-for-greater-effect-05022023.pdf

Guide to CyberCX Intelligence reporting language

CyberCX Cyber Intelligence uses probability estimates and confidence indicators to enable readers to take appropriate action based on our intelligence and assessments.

Probability estimates – reflect our estimate of the likelihood an event or development occurs						
Remote chance	**Highly unlikely**	**Unlikely**	**Real chance**	**Likely**	**Highly likely**	**Almost certain**
Less than 5%	5-20%	20-40%	40-55%	55-80%	80-95%	95% or higher

Note, if we are unable to fully assess the likelihood of an event (for example, where information does not exist or is low-quality) we may use language like "may be" or "suggest".

Confidence levels – reflect the validity and accuracy of our assessments		
Low confidence	**Moderate confidence**	**High confidence**

Zero Day RCE in NetComm NTC-221 Industrial IoT M2M LTE/4G Router

Read More →

What the cyber reforms mean for telcos

Read More →

Insights from 100 Purple

NIST Cybersecurity

Empowering organisations to manage cyber risk, build resilience and grow with confidence in an increasingly complex and challenging threat environment.

Contact us

Call us - 1300 031 274

Get in touch Report a cyber incident

Capabilities

Governance, Risk and Compliance

Security Testing and Assurance

Identity and Access Management

Network and Infrastructure Solutions

Privacy Advisory

Cyber Intelligence

Strategy and Consulting

Crisis Communications

Insights

CyberCX Intelligence Insights

Cyber Adviser Newsletter

Customer Success Stories

Cyber Security Webinars

Blog

Company

About

Careers

Newsroom

Cookie Notice Website terms of use Terms & Conditions Supplier Code of Conduct Modern Slavery

Privacy