AUSTRALIAN DEFENCE FORCE

The Looking Glass

Stupidgate: lessons from the US Discord intelligence leaks

Matthew Sussex and Michael Clarke

Centre for Defence Research, April 2023

In this issue of *The Looking Glass*, we examine the fallout from the recent US intelligence leak (dubbed ‘Stupidgate’ by one of us) that saw hundreds of classified documents circulating amongst online gaming communities, after they were allegedly posted by Jack Teixeira, a cyber defence systems journeyman enlisted in the Massachusetts Air National Guard. The revelation that such a swathe of sensitive materials had been sourced and leaked over a period of time has naturally prompted an urgent rethink of security protocols, including over who has access to classified information.

In addition to being damaging in terms of the optics (it is effectively an ‘own goal’ by the US intelligence community, given the apparent absence of covert operations by a hostile foreign power), the leaks raise questions about the tightness of intelligence sharing between allies and the information-gathering activities of US intelligence agencies – notably, amongst friends as well as adversaries. It is likely that initial fears the leaks would have more impact than the infamous Snowden Files are ungrounded. However, the ease with which a low-level US serviceman was able to access and then release such sensitive data will require a costly and time-consuming review of US data management at a time when intelligence resources are critically required to monitor and thwart myriad threats from hostile actors.

Who was the leaker, and what was his motive?

Several days of speculation over the identity of the leaker saw open-source intelligence investigations by a variety of groups – including the open-source team at Bellingcat – narrow down a list of potential culprits, until a selfie taken by Teixeira featuring the same kitchen countertop in the background of one of the leaked documents indicated he was likely responsible. The FBI, which had already been investigating Teixeira, took him into custody on 13 April at his family’s home in North Dighton, a small town in Southeastern Massachusetts.

It appears Teixeira was the de facto leader of an online community named Thug Shaker Central, which used the popular gaming server Discord. Reports differ on whether he was posting material in February 2023 or as early as October 2022. But, he appears to have shared the documents to try to boost his status among the group members, as his actions have been described as a ‘little bit of showing off’ to his friends. Members of the group began to share the materials with the community hosted by the YouTuber Wow Mao, and then they were posted to Minecraft servers. From there they quickly made their way onto an extremist chat group on 4chan, the site notorious for far-right conspiracy theories. Within 24 hours they were being circulated on the pro-Russian Telegram channel DonbassDevushka, which has been linked to the former US Navy NCO Sarah Bils.

The case is an unusual one because Teixeira appears to have been neither a foreign agent (or a proxy working on behalf of one), nor a whistleblower with a strong ideological motive to leak the documents. It is true Teixeira and other members of his Discord group were gun enthusiasts with an interest in the Russia–Ukraine war, shared racist memes and several of them were mistrustful of the US government. But Teixeira's apparent main motivation – to stand out in his online community as the 'OG' – is not one typically associated with such intelligence leaks. The cases of John Schulte (who was found guilty of sending Wikileaks information about CIA hacking tools), and Chelsea Manning (who pled guilty in a military court martial for sending hundreds of thousands of US military and diplomatic secret documents to Wikileaks) are not comparable, given both individuals were motivated by the desire to harm the US government. In fact, Teixeira appears to have changed his method of reporting leaks to his channel – from hand-transcribing them to taking copies of the documents home and photographing them – after becoming annoyed that members of the group weren't interacting with them enough. After doing so, he became regarded as a 'legend' among his community.

What was leaked? How damaging was it?

The *Washington Post* claims it has obtained some 300 documents from the leak, which is about three times as many as were previously thought to have been released. The bulk of these appear to consist of technical data and signals intelligence concerning the war in Ukraine. They do not include extremely damaging information, such as specific Ukrainian plans for its forthcoming counteroffensive against Russian forces, but they do contain details on a variety of related topics. These include:

- assessments of Ukrainian and Russian vulnerabilities
- real-time details (in February and March) of Ukrainian and Russian battlefield positions
- casualty estimates (interestingly, the casualty figures for Ukraine and Russia were crudely swapped from the original to make it appear as though Ukrainian forces had suffered heavier losses)
- assessments of the Ukrainian air defence network
- analysis of Russia's diminished ability to conduct offensive operations
- schedules for the delivery of NATO equipment to Ukraine.

Additionally, the leaked documents contained details about infighting within the Russian political elite, as well as its security services. One of these seemed to confirm the rumour President Vladimir Putin personally intervened to quell the hostility between Defence Minister Sergei Shoigu and the head of the Wagner group, Yevgenyi Prigozhin. Another contained several claims regarding doubts cast by the Russian FSB on the veracity of official Ministry of Defence casualty figures. Another document seemed to indicate Russia lacked the capability to effectively interdict Western deliveries of lethal aid to Ukrainian forces. And the leaked cache also included the Director of National Intelligence's 'Watch Report': a compilation of uncorroborated intelligence information that may be proven false. This report listed the possibility China had agreed to provide Russia with military equipment in order to assist its invasion of Ukraine. Later, however, it was revealed this had come from Russian sources, and the US Administration spokesperson reiterated there was no evidence Beijing had done so.

Further revelations from the leaks allegedly concerned US assessments of allied nations' intentions, as well as operations within them. One of these seemed to document attempts to persuade the South Korean government to provide Ukraine with arms, via the US as the middle party. This raised concerns such a move would violate Seoul's policy to not equip nations engaged in war with military hardware. Indeed, the office of President Yoon Suk Yeol called the documents 'fabricated', and noted that suggestions the US had been eavesdropping on South Korean leaders was a 'senseless lie'.

Another leaked document suggested Egypt had been secretly negotiating with the Russian government to supply it with up to 40,000 missiles, in addition to artillery shells. As reported by the *Washington Post*, Egyptian arms manufacturers were instructed to tell their workers the arms were for its own military, and that the scheme should be kept secret to 'avoid problems with the West'. Still another document suggested Israel's intelligence apparatus had revolted against Prime Minister Bejanim Netanyahu's attempts to overhaul the court system, which would have placed far more power in the hands of the ruling party. And Australia is also mentioned as a potential party affected by the leaks, with a spokesperson indicating 'concern' at the disclosure of classified information, and noting that the government was 'seeking further information'.

It is probably too early to realistically assess the damage done by the leaks. Although, it is clear they have been sufficiently embarrassing to prompt a variety of US allies to ask for explanations while simultaneously calling for calm. Ukraine – understandably, given that it is the subject of many of the documents – has gone further. Initially they called them a falsehood and suggested they were concocted by the Russian government. Later, Defence Minister Oleksii Reznikov claimed they represented a 'mix' of true and false information. And, the office of President Zelensky noted that Ukraine had already adjusted its tactical war plans to ensure the information contained in the leaks was outdated.

But there are also reports Kyiv is increasingly concerned the leaks reveal a softening of US support for Ukraine and the reappearance of a desire to provide Vladimir Putin with a diplomatic 'off-ramp' from the conflict. Given that this is likely to take the form of Ukrainian territory, it is little wonder the Ukrainian government is irritated. More broadly, in the wash-up from the leaks, Washington faces the difficult task of reassuring allies both that it is safe to share secrets with the US, and that American intelligence gathering efforts are benign.

One aspect of the leaks not yet examined in much detail is that they seem to point to quite extensive US penetration of the Russian political and military apparatus. This is damaging for Washington because it is never good practice for your adversary to find out how much you know, and it potentially exposes sources and methods. It also gives Russian intelligence agencies the opportunity to study and counter US intelligence gathering efforts in future. It is damaging for Russia too: public revelations of diminished combat power directly contradict its official narratives about imminent victory (however implausible they might be), and questions about how US intelligence agencies were able to obtain their information will vex the FSB in its attempts to uncover who and what has been compromised.

What is to be done?

The first and most obvious task here concerns a comprehensive review of how the US manages classified information: who has access to it, who can obtain physical copies of it, and how it can be shared. It is no secret that the pervasiveness of security clearances for government work in the US permit an extremely large number of individuals to access sensitive information, potentially on topics they do not crucially need to know. The fact that a 21-year-old, who only enlisted in the Air National Guard in 2019, was privy to such a wide range of information should prompt a rethink about access at the very least. The review ordered by US defense secretary Austin is a good an necessary first start.

In addition, Teixeira’s ability to remove copious physical copies of classified information should prompt an urgent rethink of security at military and other government facilities. The removal of sensitive documents has long been a problem in the US, including at the highest levels with respect to the classified information found at former President Donald Trump’s Mar-a-Largo property. But it should not be possible – or at the very least it should be made significantly more difficult – for individuals to take classified information with them off-site.

The third task the Biden administration will need to perform is damage control. Some of these efforts have been documented above, but it goes without saying this episode will undermining trust among key partners and allies. The nations affected by the leak deserve to have complete explanations of what was taken, as well as a roadmap for how the US intends to improve information security in the future.

Finally, the Discord leaks also pose significant implications for counterintelligence practice. In addition to proxies and useful idiots, efforts must now be made to monitor other potential show-offs who want to demonstrate their knowledge, regardless of the penalties associated with violating security clearances. There is the further possibility such individuals could be unwittingly co-opted by foreign intelligence services, encouraged to produce more information by those posing as earnest members of an online community. As Microsoft President Brad Smith has observed, Russian operatives have recently been focusing on gaming communities as a way to amplify information swiftly and deniably. With such communities increasingly forming part of daily interactions for Western and especially US publics, a new front in the battle to manage sensitive information has opened up. As the leaks demonstrate, it is not just spies and hackers we need to be careful of; a teenager with an Xbox can potentially be just as damaging to national security.

Further reading

Amy Zegart, ‘Everything about the Ukraine leak is incredibly weird’, *The Atlantic*, 13 April 2023. https://www.theatlantic.com/ideas/archive/2023/04/ukraine-intelligence-leak/673703/

John Askonas and Renee DeResta, ‘How gamers eclipsed spies as an intelligence threat’, *Foreign Policy*, 15 April 2023. https://foreignpolicy.com/2023/04/15/ukraine-leak-intelligence-discord-espionage-gamers-internet-online/

David Ignatius, ‘The leaked documents on the Ukraine war are chilling’, *Washington Post*, 11 April 2023. https://www.washingtonpost.com/opinions/2023/04/10/leaked-intelligence-ukraine-chilling/

Cathy Young, ‘The Discord leaks: no, Ukraine is not doomed’, *The Bulwark*, 18 April 2023. https://www.thebulwark.com/the-discord-leaks-no-ukraine-is-not-doomed/

Jack Detsch and Robbie Gramer, ‘Washington does damage control on Ukraine war leaks’, *Foreign Policy*, 10 April 2023. https://foreignpolicy.com/2023/04/10/ukraine-russia-war-leaks-classified-damage-control/

James Dettmer, ‘Leaks show US is underestimating us again, Ukraine officials fume’, *Politico*, 13 April 2023. https://www.politico.eu/article/leaks-show-us-is-underestimating-us-again-ukrainian-officials-fume/

Ken Klippenstein and Murtaza Hussain, ‘Leaked Pentagon document shows how Ukraine war is bleeding into the Middle East’, *The Intercept*, 14 April 2023. https://theintercept.com/2023/04/13/leaked-pentagon-document-ukraine-iran-war/.

AUSTRALIAN DEFENCE COLLEGE

PROPTER POSTEROS DISCIMUS

AUSTRALIAN DEFENCE FORCE