COMBINED THREAT ASSESSMENT GROUP
CTAG

New Zealand Security Intelligence Service
Te Pā Whakamarumaru

Security Intelligence Report | SIR

Report Date: 20 June 2017
Report No: DMS 6 15 587

Online extremist activity in New Zealand

Key Judgements

1. (R) Online extremism is a multi-faceted, borderless issue that crosses many jurisdictions. Successful countering of online extremism requires a coordinated approach domestically and internationally, yet competing priorities potentially generate conflicting responses between government agencies, public and private sectors, and countries.
2. (S) Security agencies have limited sight of the extent of online extremist activity in New Zealand and by New Zealanders; increasing encryption and complexity of the online environment present challenges for detection and monitoring of such activity.
3. (S) The prevalence of online extremist material and the ease with which it can be accessed has reinforced extremist ideology among the majority of New Zealand's known s6(a) Islamist extremists. Consumption and sharing of this material is widespread among these individuals.
4. (S) The online environment has greatly facilitated contact between extremists and several New Zealand-based extremists have reinforced their ideology through online connections with like-minded individuals offshore.
5. (S) Radicalisation is driven by both online and offline influences. Self-radicalisation is more directly attributable to online influences and occurs through unmediated consumption of online material consisting of both mainstream and extremist content. s6(a), s6(b)(i) [redacted].
6. (R) Low-sophistication attacks are judged to be the most likely domestic attack scenario in New Zealand, and online material almost certainly serves to raise awareness of low-capability methods and provide justification for attacks. The online environment is a ready source of instruction on conducting more sophisticated attacks.

7. (S) Over the next few years the online environment will present challenges, but also opportunities, for security and intelligence agencies. The dynamic nature of the online environment means only broad trends can be assessed with any confidence.

    a. (R) Developments in the field of encryption will continue to challenge efforts to collect intelligence on those engaging in extremist activity online.

    b. (U) Internet penetration will increase globally, and transnational extremists of varying ideologies will use the online environment as the default arena for propaganda, recruitment, communication, and planning.

    c. s6(a) [redacted]

    d. (U) The scope and variety of internet-enabled technologies will increase rapidly over time, and will present exploitation opportunities both for terrorist groups and counter-terrorism authorities.

Context and background

8. (R) The presence of extremists online reflects a global cultural norm. Most groups, including extremist groups, make use of the expansive reach of the internet and the convening powers of social media. The online environment enhances extremists' efficacy in a number of areas and poses significant challenges to counter-terrorism authorities for detection, monitoring and disruption.

9. (R) This report identifies aspects of extremist activity that are enhanced by the online environment, in the context of the New Zealand experience. These are identified as: consumption, dissemination and production of extremist material; radicalisation (including self-radicalisation) and mobilisation to violence; direction and incitement of attacks; and, recruitment and facilitation. It considers the challenges in responding to online extremism, and how online extremism may evolve in the future.

10. (S) This report draws on examples from New Zealand's s6(a) individuals of counter-terrorism security concern, most of whom are assessed as supporters of the Islamic State of Iraq and the Levant (ISIL). This may not be a true reflection of online extremism in New Zealand; as noted in the report, limited insight of the online environment is a challenge to assessing the scale, strength and nature of extremist activity in this space.

11. (R) In focusing on online extremism, this report considers only a very specific manifestation of extremism. Online extremism does not stand alone: it is a by-product of extremism in society. Successful countering of violent extremism at its societal roots would almost certainly reduce its online expression.

Terminology

12. (R) For the purpose of this report, 'extremism' refers only to violent extremism, where violence is endorsed or accepted as a means of achieving ideological goals. The report focuses on the activities of known New Zealand extremists; currently, these are s6(a) Islamist extremists.
13. (U) 'Radicalisation' is considered to be the process by which an individual may come to accept and identify with violent extremism.
14. (U) We consider 'self-radicalisation' to occur primarily through consumption of online material and in the absence of contact with other extremists, online or real world.
15. (U) The 'online environment' refers broadly to all layers and functions of the internet across all devices and platforms.
16. (U) 'New Zealand extremist' refers to individuals with New Zealand citizenship or other New Zealand residency statuses, and may be onshore or offshore.

Online extremism in New Zealand: the current state

(R) The prevalence of extremist material online and the ease with which it can be accessed, both shapes and reinforces existing ideology among New Zealand-based extremists.

17. (R) The online environment provides free production tools, decentralised and cheap distribution on multiple platforms, geographical reach, 24/7 availability, anonymity, and algorithms that direct and curate content. Nearly all New Zealand's known extremists consume and share online extremist propaganda, s6(a), s6(b)(i) [redacted].
18. (S) Online extremist propaganda is created and distributed both by members of terrorist groups and by their global supporters. Several New Zealand ISIL supporters have contributed to these processes.
    a. (S) s6(a) New Zealand-based extremists have been charged with possessing or distributing objectionable material associated with ISIL and Al Qaida (AQ).
    b. s6(a) [redacted]
19. (R) New Zealand extremists also draw on mainstream content such as media reporting to affirm extremist narratives. s6(a), s6(b)(i) [redacted].

s6(a) [redacted]

(S) Many New Zealand extremists have reinforced their ideology through guidance from online extremist ideologues and contact with offshore extremists.

20. (S) Many New Zealand-based extremists have viewed online products by extremist ideologues, but the extent and degree of influence exerted by ideologues is difficult to judge.

s6(a), s6(b)(i)

in New Zealand, only a small number of individuals specifically reference such teaching to support their extremist activity.

s6(a), s6(b)(i)

21. (S NZEO) The online environment has greatly facilitated contact between extremists. s6(a)

s6(a)

(R) The online environment almost certainly accelerates radicalisation, but the process is complex, and is driven by a combination of online and offline influences. Radicalisation does not necessarily lead to mobilisation to violence.

22. (S) The influence of the online environment on the radicalisation of New Zealand extremists is difficult to gauge. Radicalisation is a largely internal and individual process, and counter-terrorism authorities are usually unsighted on the early stages. However, accelerants of radicalisation include access to propaganda, extremist teachers and extremist peers; these are much more readily available online than offline in New Zealand.

23. (S) Radicalisation does not necessarily lead to mobilisation to violence. Most New Zealanders who have radicalised have later moderated their views without mobilising. There has not been a completed Islamist terrorist attack in New Zealand to date.

24. s6(a), s6(b)(i)

.

a. s6(a)

25. (S) Online sites established by extremists can radicalise susceptible individuals by normalizing extremist messages and excluding moderate opinions. Such sites are not necessarily linked to specific extremist groups and do not necessarily distribute material readily categorised as extremist propaganda. It is difficult to gauge the extent to which New Zealanders access or use such sites. Further, access or use is not in itself a security concern.

a. s6(a)

(R) Self-radicalisation is more directly attributable to the influence of the online environment, but is rare, and does not necessarily lead to mobilisation to violence.

26. (R) Self-radicalisation is largely an internet phenomenon in that the offline environment does not provide unmediated, single point access to material supportive of extremist narratives. However, we judge the factors that trigger an individual to engage with such material are complex, personal, and highly likely originate in their offline lives. As with radicalisation more broadly, self-radicalisation does not necessarily lead to mobilisation.

27. s6(a), s6(b)(i)

a. (S NZEO) A Christchurch-based teenager conducted an ideologically motivated act of violence in mid-2017 which did not result in death or injury. He consumed large quantities of extremist material online, but is assessed not to be in contact with extremists, in the real world or online. He has been diagnosed with a number of mental health disorders, witnessed domestic violence as a child and was socially isolated. s6(a)

(R) Online resources do not significantly enhance extremists' capability for low-sophistication attacks, but almost certainly raise awareness of such methods and enhance extremists' confidence.

28. (S) As previously noted, there has been no completed Islamist terrorist attack in New Zealand to date. The most likely scenario for a domestic attack in New Zealand is a lone actor attack using readily available weapons such as a vehicle for driving through crowds or a bladed weapon such as a knife. Such an attack is not reliant on the internet for planning or execution. However, groups such as ISIL and AQ have provided explicit instructions online for conducting such attacks and these resources almost certainly serve to increase awareness of such methods, as well as desensitising, providing religious justification, and building confidence for would-be attackers.

29. (S) Capability for planned or directed attacks using sophisticated weapons such as explosive devices or chemicals is greatly enhanced online. s6(a), s6(b)(i) many aspects of these attacks, such as identification of targets, attack methodology, weapon construction research, and direction and communication are conducted online. s6(a) New Zealand extremists are almost certainly aware of online resources for enabling sophisticated attacks, s6(a)

(S) Online incitement can generate or reinforce intent to conduct terrorist acts. A small number of New Zealanders have attempted such incitement.

30. (S) Online messages from ISIL leadership, including Abu Bakr Al-Baghdadi, deceased senior leader Abu Mohammad Al-Adnani and his replacement Abu Hassan Al-Muhajir, incite followers to conduct attacks in the West. However, NZSIS has not noted increased attack rhetoric by New Zealand extremists following such messages.

31. (S) NZSIS is aware of unsuccessful attempts at incitement by a very small number of New Zealand extremists.

    a. (R) A Syria-based New Zealand ISIL member produced a video urging New Zealanders to conduct attacks in New Zealand on Anzac Day 2015.

    b. s6(a)

(S NZEO) New Zealand was affected by ISIL's online recruitment and facilitation of Western foreign fighters to the Caliphate, but not to the same extent as Western partners.

32. (S) Recruitment and facilitation are accelerated by the online environment's ability to put recruiters and facilitators in direct contact with would-be followers.

33. (S NZEO) s6(a), s6(b)(i) . New Zealand was also significantly affected by the recruitment drive, but on a much smaller scale. NZSIS is aware of s6(a) New Zealanders that travelled to Iraq and Syria to join terrorist groups in this period, with several more being disrupted in travel attempts. It is possible some of these individuals were recruited or facilitated through online contacts, and highly likely most were recruited in the broader sense of being motivated to join through online propaganda. s6(a)

s6(a)

s6(a)

(R) Financial support to terrorists through online mechanisms has not been a significant issue for New Zealand to date.

34. s6(a)

    a. s6(a)

Key issues in addressing online extremism[1]

35. (R) Online extremism is a multi-faceted, borderless issue that crosses many jurisdictions and can generate conflicting responses. Online extremism touches on the mandates and priorities of many public and private sector organisations, locally and globally. In the absence of a coordinated and holistic approach across all parties, conflicting views and unilateral actions can undermine progress. For example, the takedown of extremist platforms may meet law enforcement or technology industry priorities but may decrease opportunities for intelligence collection or counter-messaging. The difficulty of coordination is compounded by restrictions on sharing classified information and lack of formal channels for cooperation between domestic government agencies and multi-national technology corporations.

36. (S) s6(a) Ubiquitous encryption, the rapid rate of change in online technologies, and the size and complexity of the internet, are challenges when gauging the full extent, strength and variety of online extremism, and its impact in New Zealand. It can be difficult to identify online activity as extremist given that much of it – communication, research, sharing information – resembles activity by ordinary citizens and is not in itself a threat to national security.

37. (S) Targeting extremist material as for discovery purposes is also problematic: terrorist propaganda may be used legitimately by researchers and educators, while at the same time generalist content such as media reports can be framed to serve extremist narratives.

[1] NZSIS and CTAG would not normally comment on mitigations or make recommendations, but have been specifically tasked to do so in the terms of reference for this report.

38. (S) While technical and human intelligence solutions can almost certainly be found to enhance discovery of online extremist threats, proportionality and necessity remain key to balancing security requirements with freedom and privacy in the online environment.

Outlook: future threat posed by extremist activities online

39. (R) The future direction of online extremism can only be judged in broad terms. Change is common in the history of transnational extremism, often reflecting geopolitical developments, while technology evolves rapidly and with increasing speed, making future technologies and their uses difficult to foresee. The assessments below are based on the assumption that current trends continue.

40. (R) It is likely global internet access, currently at 47% penetration, will increase. Connectivity in currently underserved regions could extend the reach of extremists, or increase the capability of extremists in such regions to undertake terrorist activities.

41. (R) It is highly unlikely that encryption will decrease, given public demand for privacy, government requirements for protection from cyber threats, and competitiveness in the technology sector. Developments in the field of encryption will continue to challenge efforts to collect intelligence on those engaging in extremist activity online. However, legislation and other regulatory mechanisms that enable government access to encrypted data under national security mandates may somewhat offset intelligence challenges presented by encryption.

42. s6(a) [redacted]

43. (R) Transnational extremists of varying ideologies will increase their online presence, and the online environment will be the default arena for activities of security concern: propaganda dissemination, recruitment, facilitation, target research and attack planning will increasingly occur online, through encrypted channels. While Islamist extremism will likely continue to be the dominant transnational counter-terrorism threat over the next few years national security threats from other groups may increase, and these groups will almost certainly operate online.

44. (R) Cyber-terrorism capability among transnational terrorist entities is currently assessed as rudimentary, but will possibly increase, although likely at low-level capability. Appetite for cyber capability among extremists will likely grow as critical services such as power supply and financial institutions are increasingly managed online. Disruption of these services in a Western country would be seen as a desirable target for terrorists, and it is possible targets will be chosen opportunistically, based on weakness in security.

45. (R) The scope and variety of internet-enabled technologies will increase rapidly over time and will present exploitation opportunities both for terrorist groups and counter-terrorism authorities.

ENDS

NZSIS Contact: Intelligence Publications Manager s6(a) [redacted]

Distribution

s6(a)

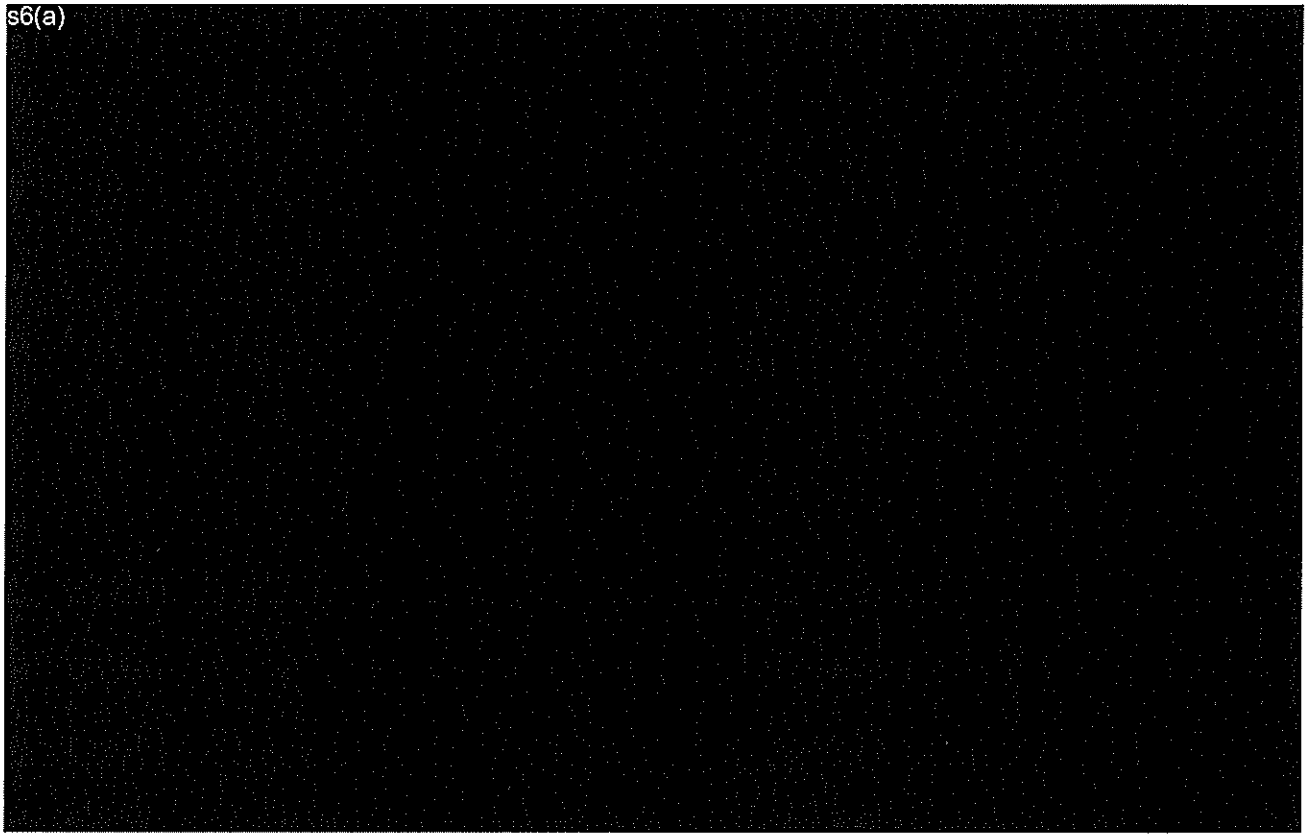
HANDLING AND SECURITY INSTRUCTIONS

GENERAL

This report is issued for intelligence purposes only, and remains the property of NZSIS. No action may be taken on this intelligence without prior reference to the originator. This intelligence MAY NOT be used evidentially.

This report MAY NOT be distributed to, nor may its contents be discussed with any person who is not authorised to read SIR reports at the appropriate level (SECRET or TOP SECRET), unless the consent of the originator has first been obtained. It also MAY NOT be passed to other Departments, but the originator will consider promptly any request for additions to the distribution.

s6(a)



EXTRACTING AND COPYING

If the originator has agreed that a Department may extract or copy SIR material for collation files, the files concerned MUST be accorded the same protection in all respects as the original material. Each extract must show clearly the reference number, date and security grading of the original report, together with all caveats and handling restrictions. Requests for additional clean copies of SIR reports may be addressed to the originator. In addition to the above, this material may be incorporated into electronic systems so long as those systems are accredited at the appropriate level (SECRET or TOP SECRET) and fully protected against unauthorised access.

ATTACHMENTS

Photographs, plans, sketches and tables attached to SIR reports MAY NOT be reproduced without the consent of the originator.

s6(a)