
# Cyber

## #MH17: Initial observations of Russian influence operations relating to Australia

**Joint Standing Committee on Electoral Matters, Parliament of Australia**

**Inquiry into and report on all aspects of the conduct of the 2016 Federal Election and matters related thereto**

**Submission on notice**

Tom Sear, UNSW Canberra Cyber

# #MH17: Initial observations of Russian influence operations relating to Australia

Tom Sear, UNSW Canberra Cyber

**Joint Standing Committee on Electoral Matters, Parliament of Australia**

**Inquiry into and report on all aspects of the conduct of the 2016 Federal Election and matters related thereto**

**Submission on notice**

## Executive Summary

Australian democracy functions within a digital information environment where citizens are confronted by threat actors with a global reach, in an era of persistent long-term state competition. Initial analysis suggests that, in this new environment, Australia's actions in the international community might correlate with activity from adversarial actors in online media used by Australians.

In an internet where a revisionist power can easily reach into Australian society online, it is likely adversaries will experiment with influencing discourse generally as well as psychographically, targeting individuals and groups associated with interest groups and, potentially, populations associated with cyber vulnerable minor parties. This report explores one particular example of international concern, style of interference, and nation-state actor: Russian-generated social media activity around the downing of Malaysian Airlines Flight 17 (MH17).

Early data implies that Australian military and diplomatic efforts might have correlated with increasingly coordinated interventions into Australian political social media. Australian responses to the downing of MH17 may have seen – admittedly, minor - interference in Twitter #auspol and Australian topic content from known disinformation operations. It is wise to be cautious and not overstate either the scale or the effect of these measures. However, when they are known to operate amongst a broad spectrum of coordinated efforts, it may be worthwhile the Australian Government explore ways to monitor and check these emergent effects.

While these interventions have been comparatively small, they require an agile ongoing response and situational awareness from government. Current Commonwealth arrangements are not well configured to deal with tactical or strategic information operations in our democracy. A sustainable interoperable, interagency whole of government response is required.

## Background/Context

### Overall

As the companion submission to the committee with this document, 'Swimming between the flags' (Sear, 2018) demonstrates, the internet has transformed politics, and social media influences how political discussion takes place. State-driven information and influence operations are being carried out on a scale never before experienced.

The purpose of this short study is to demonstrate how one form of integrated strategy from a foreign actor might be expressed in social media relating to Australia. Specifically, does targeting Australia in general correlate with MH17 related actions that might be perceived as negative to the Russian Federations view of the MH17 incident?

*Russian Activities and Intentions*

In February 2018 the courts in the United States charged Russian organisation the Internet Research Agency (IRA) with 'operations to interfere with elections and political processes.' The IRA created at least 3841 fake Twitter - often called 'troll' - accounts and used them in a coordinated information operation with the aim to influence politics and public opinion in multiple countries from 2014-2017.

The US Office of the Director of National Intelligence found with a high confidence that Russian military intelligence (General Staff Main Intelligence Directorate or GRU) was part of an influence campaign which :

> followed a Russian messaging strategy that blends covert intelligence operations such as cyber activity with overt efforts by Russian Government agencies, state funded media, third party intermediaries, and paid social media users or "trolls." (ii).

This strategy is commensurate with a wider Russian Federation doctrine where the 'main battlefield is consciousness' and whereby, through undermining democratic norms and institutions, 'subversion is not the prelude to war, but the war itself'.

It is important to understand that social media intervention does not occur in isolation. Interventions in Australian social media are likely to exist on a spectrum of measures associated also with kinetic deployment of assets in the air, and electronic and information warfare measures in the Syrian conflict. It is possible these interventions occurred coincident with MH17 related active cyber measures against the Australian Defence Force (ADF) from 2014. The contribution of Australian-based military sites to shared intelligence of the Eurasia region would also make Australia an ongoing intelligence target for the Russian Federation.

*Malaysian Airlines Flight MH17 Incident*

On 17 July 2014, Malaysian Airlines Flight MH17 was bought down over eastern Ukraine. 283 passengers and 15 crew were killed. 196 were Dutch nationals and 38 were Australian. Extensive international collaborative investigations and diplomatic efforts including Australia subsequently occurred 2014-17, and are ongoing.

Following extensive investigation the Netherlands and Australia have held Russia legally responsible for its part in downing flight MH17. A Joint Investigation Team (JIT) composed of justice authorities of Australia, Belgium, Malaysia and Ukraine announced on 24 May 2018 that the Buk missile installation that brought down the flight belonged to the Russian army.

A joint international open source investigation led by OSINT organisation Bellingcat conclusively identified in May 2018 that a high ranking officer of the GRU was integral to the delivery of the BUK missile which brought MH17.

Evidence that the GRU is connected to the MH17 incident is important because, as US intelligence services indicate, the GRU is connected with the strategy for IRA actions. Flight MH17 was brought down on July 17, 2014. The following day, July 18, 2014, is the biggest single day in terms of volume in IRA tweets. The sheer volume of activity is massive and bears no relation to any other day in the

entire set. It is possible that the GRU advised the IRA that it was an 'all hands on deck' day to 'flood' social media and 'Astroturf'. On July 18, there were 57,646 tweets, July 19, 41,148, and 11-18 August, the volume was high as well.(see Figure 1) [1] Astroturfing is well known propaganda tactic to simply swamp social media feeds and prevent news, theories and outrage, getting out of hand. It is an attempt to install a kind cognitive tax on users who are then unable to focus and enable a message or crisis to escalate.

MH17 was topic in the Australian Twittersphere through which the IRA disinformation approaches sought to twist and distort opinion and plant conspiracy theories to misdirect a user's opinion away from Russian guilt. A very recent Dutch study revealed findings which are very similar to those presented here. The Netherlands was a key collaborative partner in the investigation and diplomatic efforts associated with MH17. The Dutch investigators found the Netherlands were of limited interest as targets to the Russian Trolls aside from MH17 and their leader Geert Wilders. The MH17 set, aside from the possible astroturfing exercise above, was not a large volume of total tweets. IRA Twitter accounts tweeted only 1400 times about MH17 according to the Dutch study. (Concurs with data in Figure 3). This is minuscule proportion of the total 9 million messages sent. But our focus here is *how* and *when* Australia was targeted. The Dutch team found 2693 tweets with the keyword MH17. The first was sent on July 17, 2014 and the last May 28, 2018. The most shared (283) was written in Russian, occurred on 28th of September 2016 and the text of this tweet stated: 'Main conclusion of the MH17 report: we point out the Russian side as guilty, but as long as we do not have all the details, wait until 2018.' The second with 45,000 followers stated 'The MH17 is shot above the village of Grabovo, who has brains in his head and does not understand sawdust that Ukraine has him shot.'(Translation from Russian).

In response to the MH17 incident the Russian Federation deployed a cold war style disinformation campaign, but through the rapid response, dissemination capacity of the internet. The first action was to blanket deny any involvement and an aggressive 'assault' on the MH17 Wikipedia, in an effort to persistently remove any mention of Russian culpability. Subsequently via official media stories were spread which sought to blame the Ukrainian government, the Malaysian airline and allege that Russia was the victim of smear campaign. Later, false and sometimes contradictory visual evidence, from alleged satellite images and doctored photos was spread online as part of no less 6 theories of why the downing of MH17 occurred.[2] Singer and Emerson sought to test the capacity of the Russian disinformation campaign to respond to MH17 three years after the event.[3] The authors created a 'Honeypot' by posting a Bellingcat MH17 report online. Within a few minutes a previously unknown account spammed them with messages disputing the claim. This was akin to myself and Mike Jensen's experience in Australia recently. When some initial findings were posted online in less than an hour of the story appearing, the comments section 'below the line' was subject to overwhelming spam, suspicious links, and abusive comments indicative of Russian troll activity from completely new profiles. Some of these comments are are reproduced in Figure 8.

[1] With thanks to Dr. Michael J. Jensen Senior Research Fellow, UCIGPA, University of Canberra for this observation, provision of statistics and Figure 3.
[2] See P.W. Singer and Emerson T. Brooking., *Likewar: The Weaponization of Social Media*., Houghton Mufflin Harcourt, New York., pp. 109- 110. See also pp. 70-77.
[3] See, Singer & Emerson., p. 115.

If information war, and its close association with cyber measures, are about the 'contest for the provision and assurance of information to support friendly decision-making,'[4] then a democratic society's social media environment is part of that environment.

The question then arises: Did Australian political, diplomatic and military actions in response the downing of flight MH17 result in a coordinated effort to interfere within the Australian political social media environment?

## Research methodology and findings

*Hypothesis and Method*

This brief study commenced with the hypothesis that the IRA and GRU actively responded (in however minor a way) either preceding - on - or subsequent to, Australian diplomatic activities and inquiries into the events of the MH17.

Figures 1-3 time series were extracted from the entire dataset time series from the Twitter release of October 17, 2018 available here. These three figures were generated by and are supplied by my research colleague Dr Mike Jensen at the University of Canberra.

Figures 4-7, the time series charts, pie charts and network map arise for the July 31 FiveThirtyEight data set released from Clemson University available here. These figures arise using software created by Peter Kimberley of Gradata Systems who has produced these reports at my request. These figures tentatively explore the network qualities of accounts associated with the Australian targeted MH17 and #auspol tweet set that are included in Figures 1-3.

*Key Dates: Flight MH17 incident and response*

The key dates of activity which are explored in the figures include:

- July 17, 2014. Downing of Flight MH17.
- July 25, 2014. Prime Minister Abbott confirms troops will be sent to Ukraine.
- July 17, 2015. A video obtained by Australian media shows a separatist looking at wreckage
- July 29, 2015. Russia vetoes a UN Security Council resolution drafted by Australia and partner countries to set up international tribunal for prosecution.
- October, 2015. The Dutch Safety Board (OVV) investigation is released
- Sept 27, 2016. Russia release radar data on supposed Ukrainian complicity in downing MH17
- Sept 28, 2016. International criminal investigation team determines Buk had been brought from Russia to Ukraine.
- July 17 each year (2015-17) on commemoration of downing
- July 5, 2017. Australia joins Joint Investigation Team (JIT)
- Sept 20, 2017. JIT MOU signed at the UN

*Data*

As already discussed Figure 1 illustrates the how MH17 incident was the impetuous for large scale IRA activity. There was a huge spike on July 18 2014, the day immediately after the downing of the passenger aircraft. The Dutch investigation found the first MH17related tweet on July 17 itself. While – as Figure 3 reveals – MH17 itself as the specific content of tweets was comparatively low, the overall

[4] Morgan & Thompson, footnote number 15, https://www.csis.org/analysis/information-warfare-emergent-australian-defence-force-capability

effect on this day may have been related to another well-known propaganda technique - flooding and astroturfing to keep distract and diffuse other content the perpetrator does not want user to see. Other overall spikes in IRA activity also occur in August-September 2015 and September 2017 (See Figure 3). These may correlate with attempts to flood during two key actions of nations investigating the downing of MH17 at the United Nations (see dates above).

Figure 2 is a time series which indicates the levels of activity of the IRA accounts focussing upon what might be identified as 'Australian' cultural and political issues, events and attempts to gain followers. It might be that the spikes in January and February each year are closely associated with the Australian Open and Russian tennis player, Maria Sharapova (including failing drugs test at the Australian Open in 2016). The latter is plausible based on an exploration of the hashtag composition of larger IRA tweet set overall (Figure 7) which finds 'sports' as a focus, at least as large as 'politics' and close to scale as 'news'. Sport would seem a sensible way to target an Australian online population. Attempts to gain followers in a populations are often not around politics, but other topics, such as entertainment. The largest single spike, in February 2017, is what Dr Jensen has identified as a 'hashtag game' to seek to involve Australian followers.[5]

Figure 3 is a time series of all Internet Research Agency (IRA) tweets with: Auspol, MH17, and Australia mentions. These are staggered and aggregated by week. Annotations to this figure (numbers 1-8) show the possible correlation with these three mentions and MH17 downing and diplomatic response events. The focus of speculation here is to explore tactics like flooding indicated above and it would seem clearly connected to July 18 overall. There are some correlations with most of these events. For Australian activity there is some possible temporal correlation with the events of July 2015 in the Australian media, domestically and the UN. However, perhaps of most interest is that while the correlation is both very small and loose throughout 2014-2018 there does seem to be a more organised and tighter grouping of activity around or leading up to September 2017 when Australia signed the MOU with the Joint Investigative team very publically at the United Nations.

How then did these accounts aim to create influence? Figure 4 takes these three thematic groupings and explores the IRA user accounts which most activity pursued these themes in their tweeting activity. Figure 4, shows IRA tweets (and the account which tweeted them) with any of the hashtags 'auspol', 'australia', or 'mh17' (but necessarily all three at once).[6] These are reflective of which troll accounts mention MH17, who have also been tweeting about auspol and Australia. The chart, top left, shows these and other hashtags from those tweets over time. The table top right shows a sample of these tweets. The pie chart bottom left shows the proportion of tweets from which account are evident. The pie chart, centre bottom, shows other hashtags associated with these tweets. The hashtags from these accounts when tweeting on these issues do show hashtags which might be expected with MH17 disinformation included 'boeing,' 'netherlands' etc. However, it is surprising to see very specific knowledge of the Australian political Twittersphere with hashtags such as #qldpol included.

---

[5] Personal discussion with Dr. Michael J. Jensen Senior Research Fellow, UCIGPA, University of Canberra for this observation. Tentative observation at this time. Examples of Tweets Dr Jensen has found include: "@AIDEN7757: Gallipoli of Thrones #MakeTVShowsAustralian", "@ERICARUTTER: Sheila the explorer #MakeTVShowsAustralian", and "@CALEBPAAR: American Drongo #MakeTVShowsAustralian"

[6] An example of IRA tweets which contain #auspol, #Australia #mh17 would be from account handles '@SCREAMYMONKEY' and '@SPECIALAFFAIR' in May 2016: 'Australian firm names Russia, Putin in MH17 compensation claim'. Like the Netherlands IRA #auspol tweets often targeted the leaders, such the PM, such as '@ALFREDTHREE: Tony Abbot used and manipulated terror threat as a political weapon' or the Government '@ADRIENNE_GG #My4WordNewYearsResolution. Give The Government Hell. #AusPol.'

Of note, in the time series top left, is the distinct spike of combined activity (however small) around and prior to September 2017. This mirrors observations made above about Australian UN activity(See Figure 3). This spike in September 2017 may also suggest that rather than specific targeting of Australian Twittersphere per se, there is also an attempt to 'internationalise' the MH17 response from the IRA.

Figure 5 shows the network of IRA troll accounts. The figure shows network graph of troll accounts which tweeted with any of the hashtags 'auspol', 'australia', or 'mh17'. This is reflective of which troll accounts mention MH17 and who have also been tweeting about auspol and Australia. While it is clear that many accounts touched upon the topic, some accounts (those clustered in the centre of the diagram) did focus on actioning influence across all these fields and perhaps the Australian Twittersphere more generally.

Figure 6 shows network graph of troll accounts which tweeted with any of the hashtags 'auspol', 'australia', or 'mh17' (very few tweets) (like Figure 5) and looks at what other hashtags were most frequently being used by each of these troll accounts. From this we can observe that, even though their activity in Australia was small, one goal was to be influencing opinion in issues like 'syria', 'aleppo', 'merkel', 'isis' and of course, 'sports'. So, once again, while influence in the Australian Twittersphere was small, there is evidence of troll accounts attempting to draw Australian followers into a wider global sphere of issues and debates, and vice versa.

**Implications and Interpretation**

There is a strong correlation between the downing of MH17 and involvement from the GRU, and the July 18, 2014 IRA overall activity spike indicates the commencement of widespread online activity from Russian influence actors.

This study finds a *possible* – albeit weak – correlation in the IRA Troll activity with Australian-themed content, auspol and MH17 in relation to some diplomatic activity instances - in particular July 2015 and September 2017. These correlate with Russian veto of a tribunal, when Australia joins the Joint Investigation Team (JIT) and the JIT MOU is signed at the UN. There is a possible temporal correlation with events associated with MH17 diplomatic and inquiry events. This may constitute efforts to shift opinion around or about these events and MH17. Equally this may attributable to another, completely different and unknown factor and could therefore be pure coincidence.

Note this is correlation not necessarily causation and the numbers are minuscule in comparison with other efforts at influence. The likely impact of this intervention in the Australian Twittersphere upon Australian opinion is unknown.

What is significant is that this might have been a part of a much wider coordinated effort between GRU, IRA and Russian diplomatic actions at the UN, and fake news initiatives reflected in these correlations. Of greater concern is the possible increase in organisation as time progressed. The increasing closer correlation as time and diplomatic events escalated 2014-2017 might suggest a closer integration between strategic and tactical information and cyber measures from an adversary.

This is important because rather than being associated with elections, this data reveals a pattern of consistent, continuous action commensurate with Russian Information War efforts. It is important not to ascribe IRA-related activity with excessive effectiveness or levels of influence it does not deserve. However, what is evident is persistence and consistency through a long temporal scale. This means that when Australian Government diplomatic, military and cyber measures take place the Government

would be well advised to maintain situational awareness of the pattern of response from state-based influence actors online, in social media and direct targeting as part of normal activity.

However, it is also critical to understand that each state-based influence strategy is different, and will required different kinds of monitoring and response. This is because tactics and strategy for information operations between Russia and China differ (see, 'Swimming between the flags' Sear, and 'How digital media' Sear et.al., related submission to Committee Nov 2018). Chinese Government influence, for example, is more complex. The general reasons for Russian – chaos effect seeking measures – example, as extrapolated here, are clear cut. Also Russian Federation and IRA operations tend to exploit US-based social media. Alternately, Australia experiences electronic 'entanglement' with China, with influence flowing through Chinese-centric media consumed by its diaspora. These media are likely near diaspora saturation and may possibly have up to 600,000 followers per Australian based 'Official Account.' This means that expeditious examination of how Foreign Influence Transparency Scheme Act 2018 is applied and enforced with reference to Chinese language social media in Australia will be important. It may be wise for the AG, ACSC, DFAT, ASIC, ASD, Home Affairs and the AFP actively pursue these concerns rather than passively expect reporting.

**Recommendations and actions**

What is described here is minimal. However, this may be a forewarning of future operational activity and it may be wise to be ready.

The Australian Government structures charged with responsibility for this situation are not currently designed to respond such threats.

Integration, interoperability, and interagency efforts which maximise a 'Whole of Government' approach are required to effectively meet the new normal' of competitors interfering in Australian political social media continuously. We need to be able to anticipate, identify and respond to activity in real-time.

This might include an ongoing, sustained entity which analyses and provides Government with situational awareness of real-time cross platform activity. Agencies incorporated might include a shopping list such as: ACSC, DFAT, Home Affairs, AEC, ASD, ASIO, AFP, ADF(IWD), AGs, Finance, ASIC, PM&C, ONI, NSC, Energy. Coordinated effort will guarantee effective response and minimal redundancy. Revisionist powers operate in the grey zone, we also must share ambiguity, to control the threat.

It is likely that this group could provide preparation towards contingencies arising from protracted and complex, multi-vector, multi-wave, multi-theatre attacks against cyber assets. Russian active measures on critical infrastructure have been documented. Such assets might include Australian critical civil infrastructure. Any such event would likely be combined with a spectrum of information operations in Australian social media. As such this group should provide regular simulation and briefing exercises for State level, police, SES and health services in urban environments, and understanding the information layer of cities as also composed of a network of internationally connected and enabled actors. In addition, critical infrastructure services should be incorporated within communication and contingency planning strategies.

Any such government taskforce group would be required to ensure close working collaboration with international tech and social media corporations towards close, near real-time and long term data sharing arrangements.

Leverage relationships with Five Eyes partners as force multipliers to ensure intelligence sharing and capability building.

Legal and governance arrangements and a cycle of Russian and Chinese efforts to contest information norms in global forums necessarily place Australia at a disadvantage. Adversaries do not possess our limitations. WoG effort must acknowledge DFAT cannot be expected to address all current adversarial Information Operations in Australian online media arising from issues associated with Australian participation in military interventions and peace missions. Equally, addressing competitors and influence interventions must include aggressive diplomatic efforts.

Our efforts to build resilience in the Australian public engaging online will also require knowledge of the cultural capabilities that make Australian society 'Antifragile,'[7] while remaining conscious of shifting group identities and also how global societies perceive, contest norms and respond to persistent disorder.

**SUMMARY**

Analysis of tweets relating to MH17 suggest that influence operations from foreign actors could be related to Australian diplomatic and military efforts.

Foreign influence operations are not solely focused on the election cycle, but are continuous and responsive to international activity and events.

The most effective response to these threats will be coordinated information sharing and real-time capacity to identify, analyse and counter continuous threats.

[7]Nassim Nicholas Tale., *Antifragile: Things That Gain from Disorder*., Incerto, Random House, New York, 2012. My PhD thesis considers that the Australian tradition of Anzac may be a form of Antifragile political culture. Especially when tied to volunteer cultures of participation.

**Figure 1, Time series of all Internet Research Agency tweets (IRA), Source: Twitter released data set, Oct 2018.
Courtesy Dr. Michael J. Jensen Senior Research Fellow, UCIGPA, University of Canberra.**

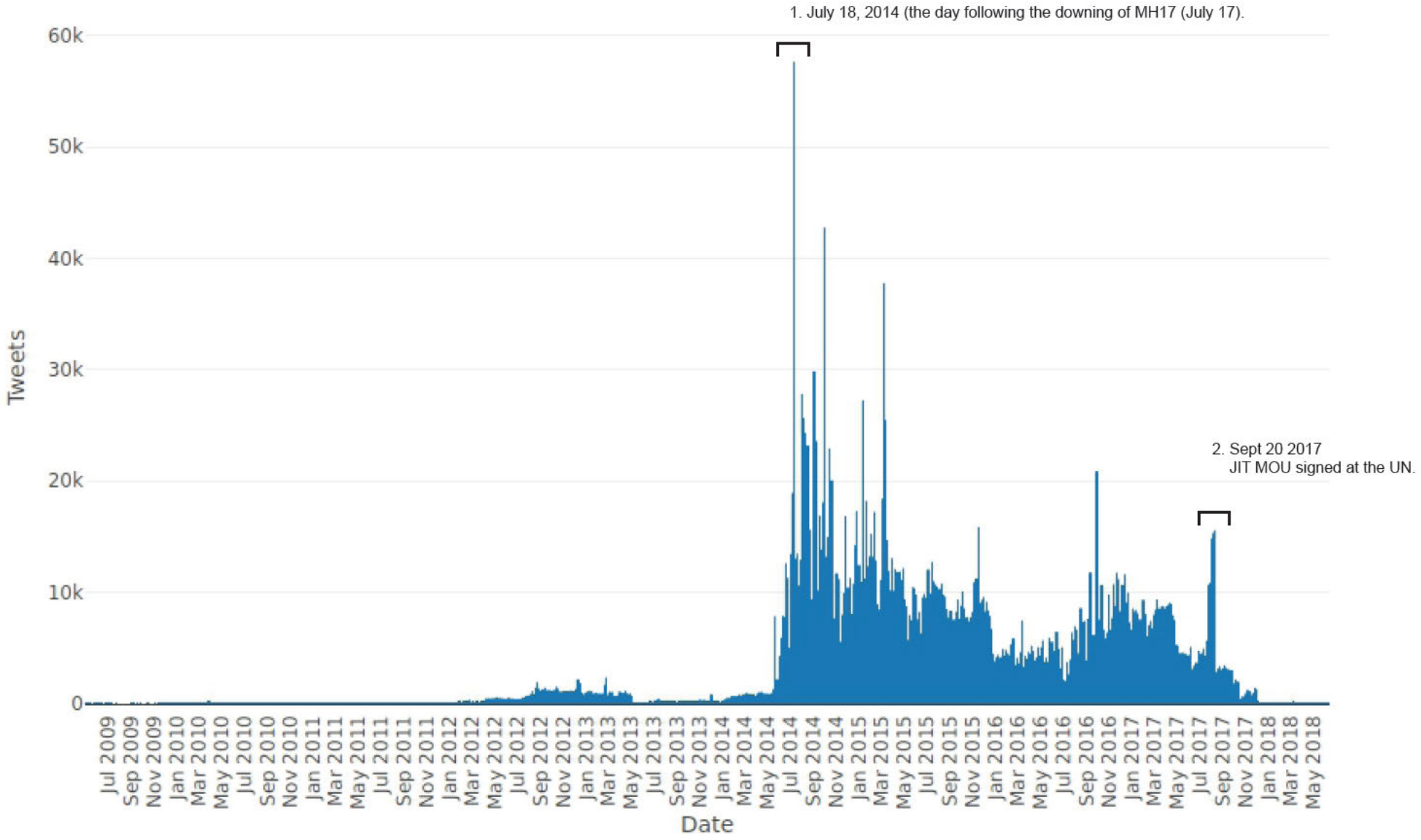


**Figure 2, Time series of all Internet Research Agency tweets (IRA) which make reference to 'Australian' based themes or ideas, Source: Twitter released data set, Oct 2018. Courtesy, Dr. Michael J. Jensen Senior Research Fellow, UCIGPA, University of Canberra.**

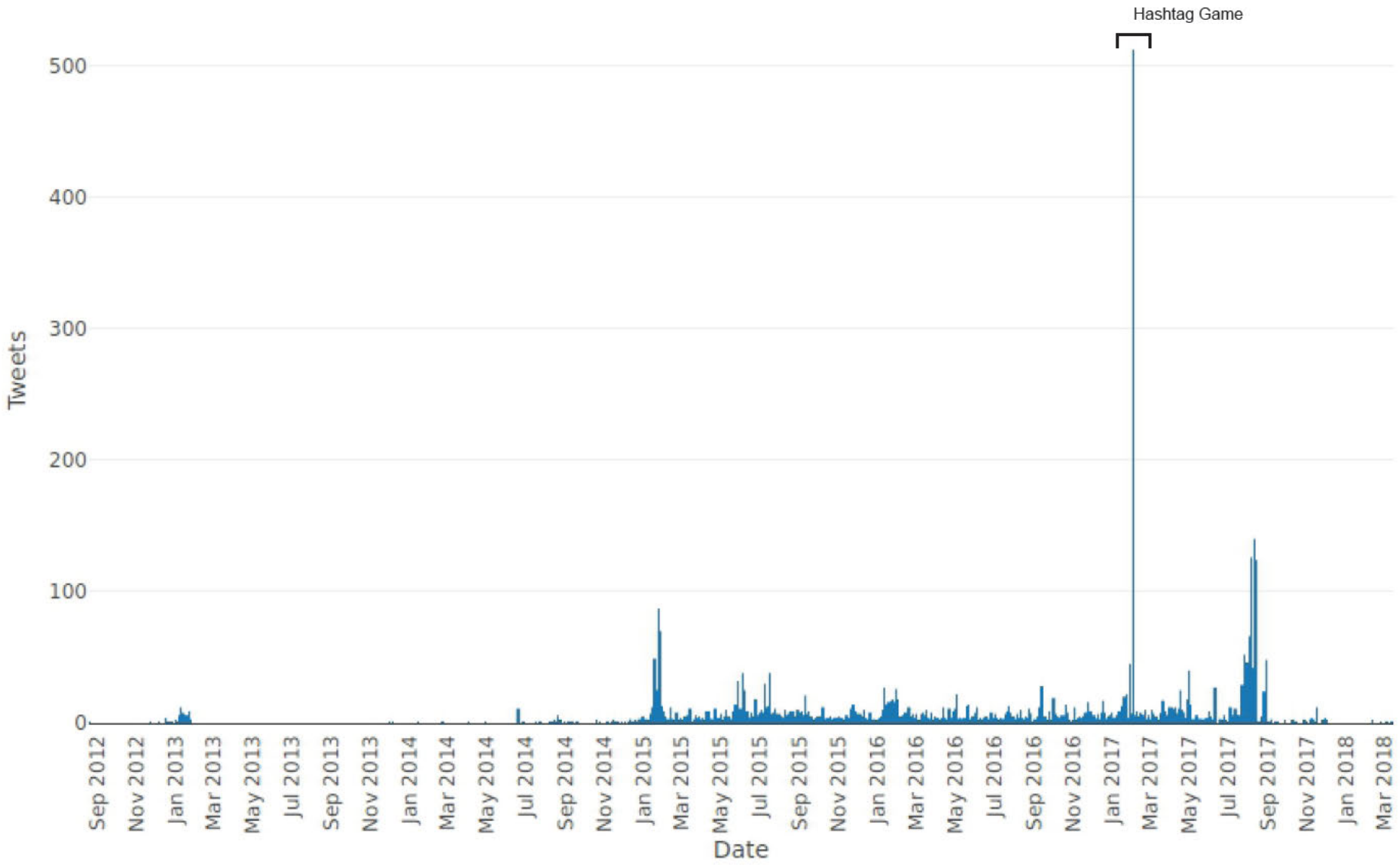
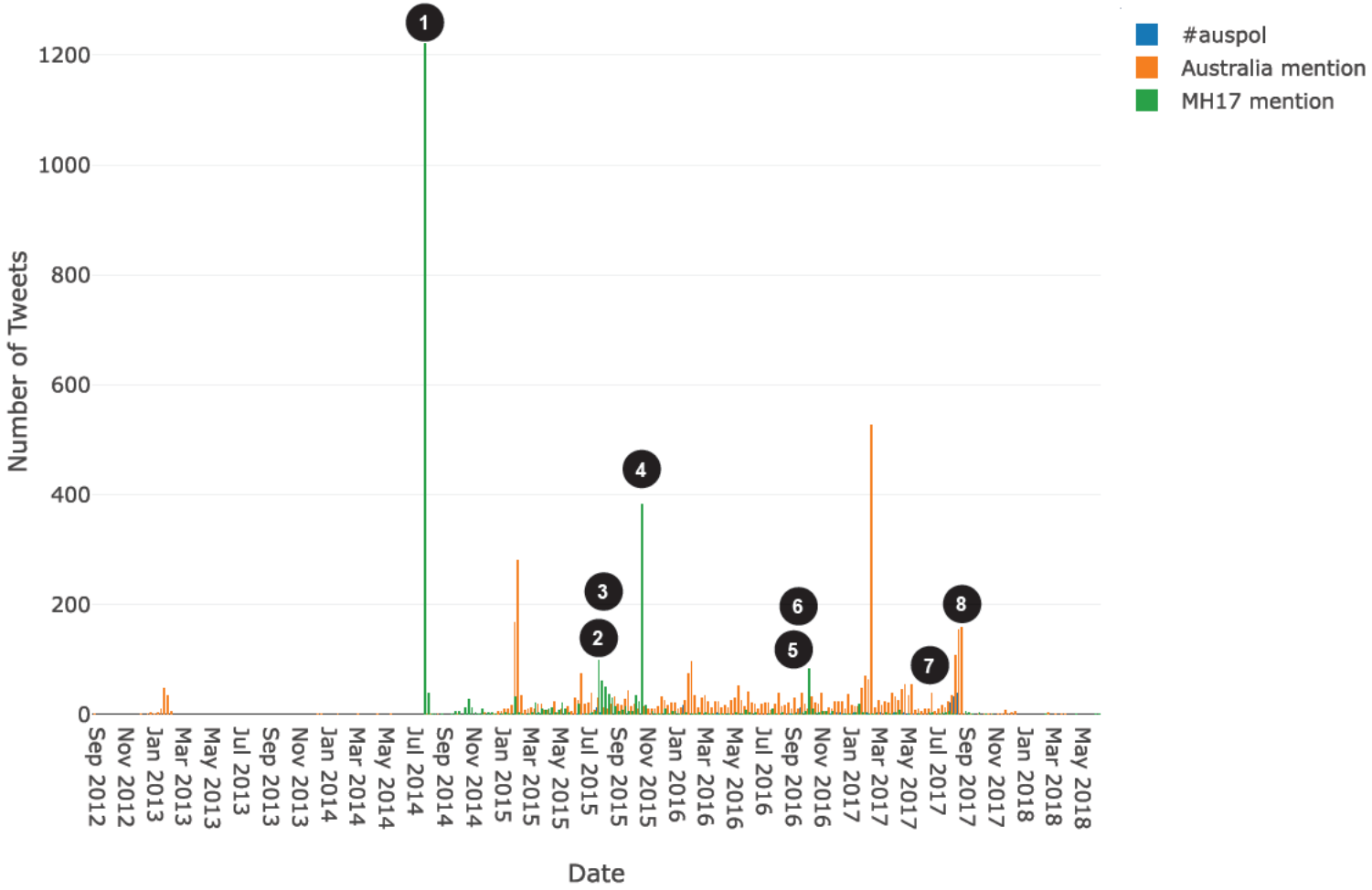


**Figure 3, Time series of all Internet Research Agency (IRA) tweets with: Auspol, MH17, and Australia mentions. These are staggered and aggregated by week. Source: Twitter released data set, Oct 2018. Courtesy Dr. Michael J. Jensen Senior Research Fellow, UCIGPA, University of Canberra.**




1. July 18, 2014 (the day following the downing of MH17 (July 17).
2. July 17, 2015. A video obtained by Australian media shows separatist looking at wreckage
3. July 29, 2015 Russia vetoes UN Security Council resolution drafted by Australia and partner countries to set up international tribunal for prosecution.
4. October 2015 The Dutch Safety Board (OVV) investigation released
5. Sept 27 2016 Russia release radar data on supposed Ukrainian complicity in downing MH17
6. Sept 28 2016, International criminal investigation team determines Buk had been brought from Russia to Ukraine.
7. July 5 2017 Australia joins Joint Investigation Team (JIT)
8. Sept 20 2017 JIT MOU signed at the UN

**Figure 4, Time series of Internet Research Agency tweets (IRA). Chart shows hashtags over time. Chart shows tweets with any of the hashtags 'auspol', 'australia', or 'mh17' (but necessarily all three at once). Reflective of which troll accounts mention MH17, who have also been tweeting about auspol and Australia. Source: Clemson released data set 2018. Software courtesy Peter Kimberley, Director: Gradata Systems https://gradata.com.au/**

**Figure 5, Network of Troll accounts, Internet Research Agency tweets (IRA). Chart shows network graph of troll accounts which tweeted with any of the hashtags 'auspol', 'australia', or 'mh17'. Reflective of which troll accounts mention MH17, who have also been tweeting about auspol and Australia. Green circles: mh17, Australia, auspol. Source: Clemson released data set 2018. Software courtesy Peter Kimberley, Director: Gradata Systems https://gradata.com.au/**

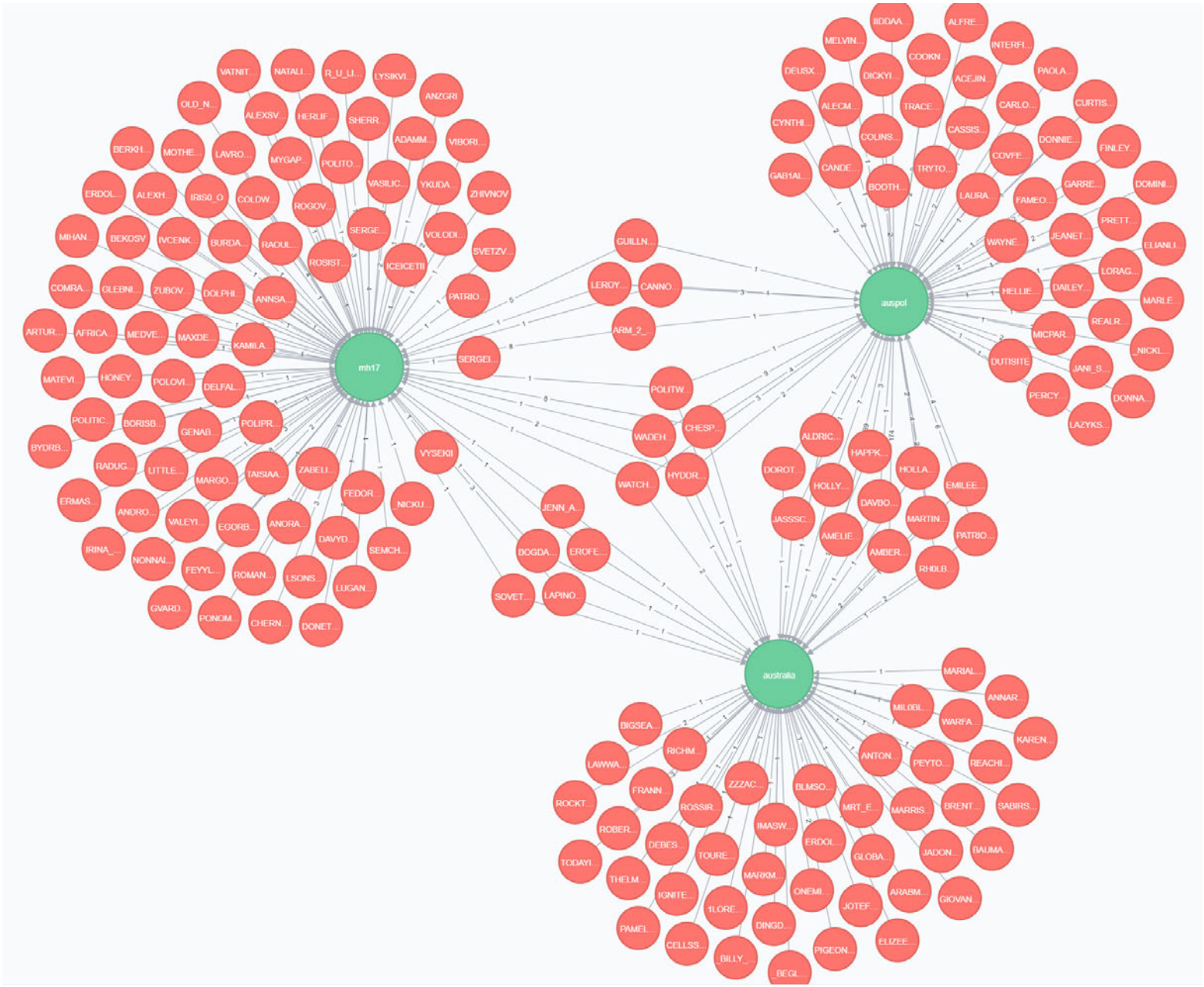


**Figure 6, Network of Troll accounts, Internet Research Agency tweets (IRA). Chart shows network graph of troll accounts which tweeted with any of the hashtags 'auspol', 'australia', or 'mh17' (like Figure 5) and looks at what other hashtags were most frequently being used by each of these troll accounts in the complete Clemson data set. Users shown are those most prolific tweeting against MH17 hashtag. Source: Clemson released data set 2018. Software courtesy: Peter Kimberley, Director: Gradata Systems https://gradata.com.au/**

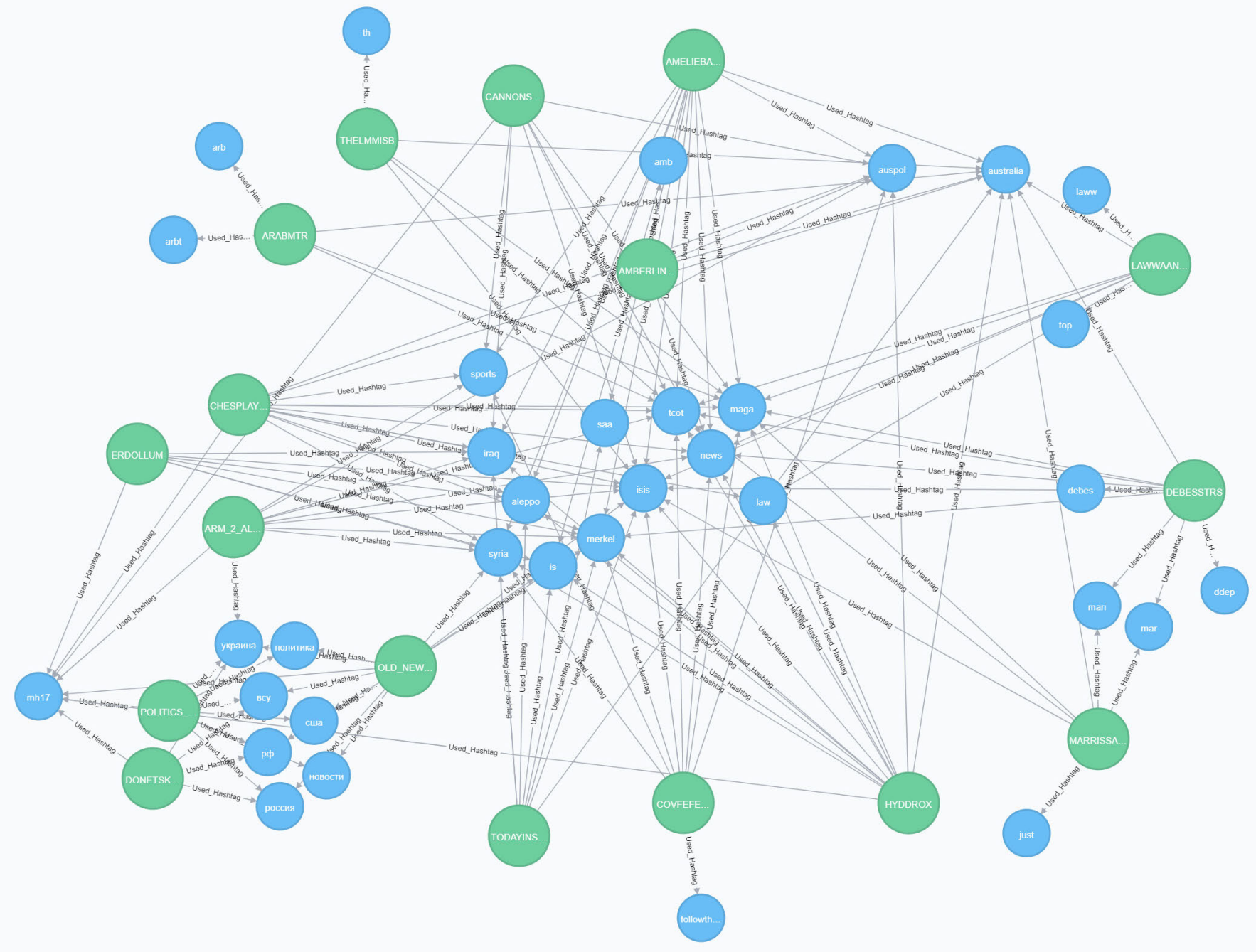


**Figure 7, Pie charts and hashtag sample , Internet Research Agency tweets (IRA) tweets: Hashtag sample Clemson set. Pie charts shows the hashtag makeup of a tweet set.
Some of these selected users are included in the mh17, Australia, auspol set. Provides illustration of the content makeup of tweets. Data table shows example of tweets ftom a user account in other Figures.
Source: Clemson released data set 2018. Software courtesy: Peter Kimberley, Director: Gradata Systems https://gradata.com.au/**

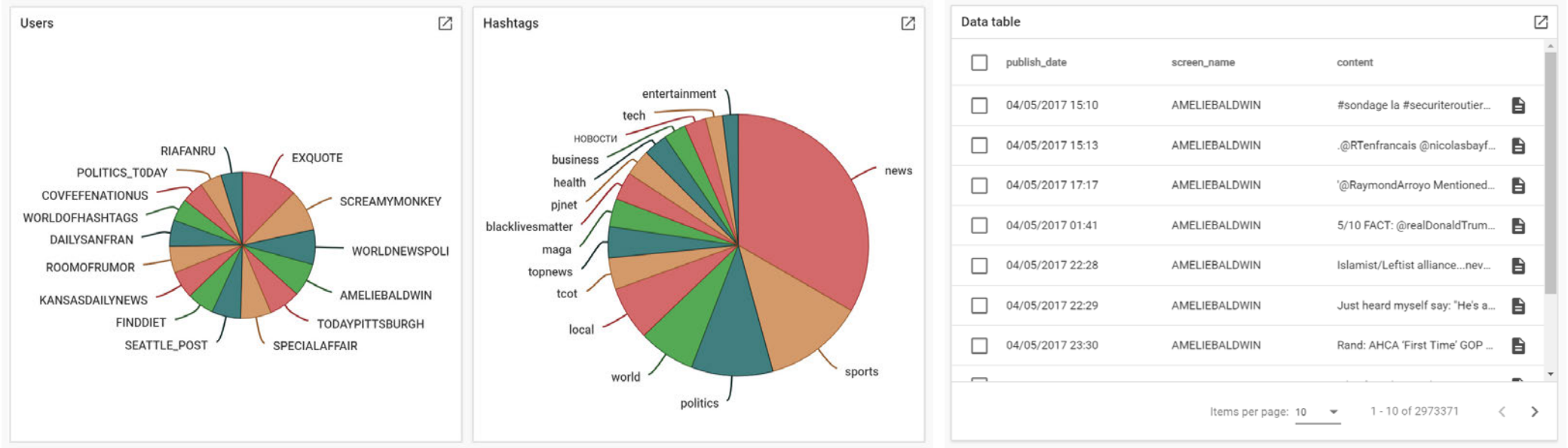
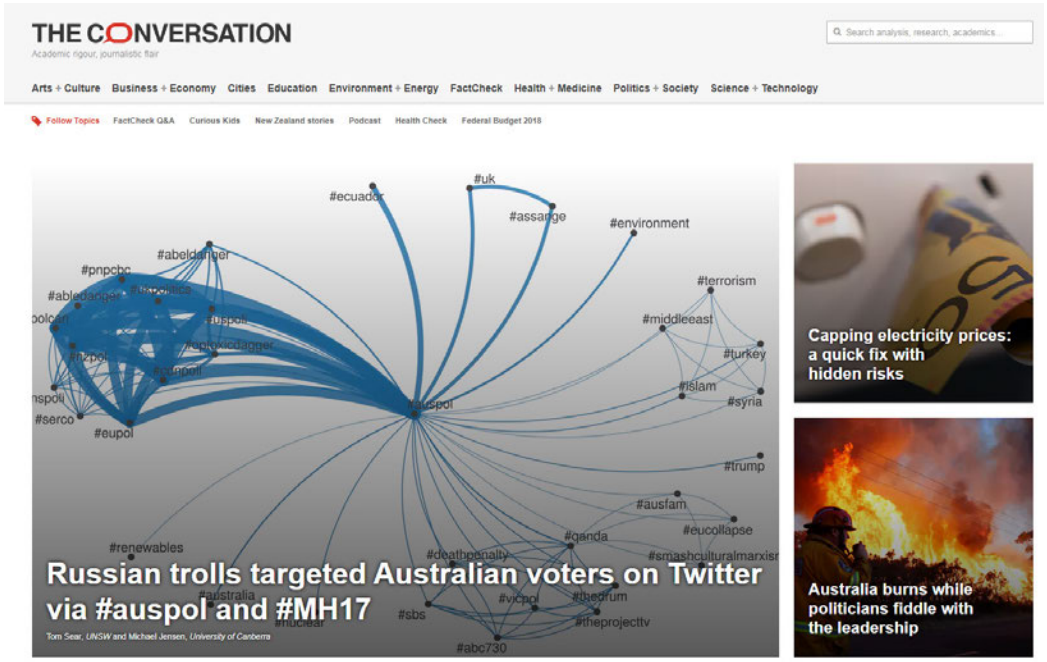


**Figure 8, Suspicious comments which appeared immediately following publishing of related article in Australian online media.**
https://theconversation.com/russian-trolls-targeted-australian-voters-on-twitter-via-auspol-and-mh17-101386

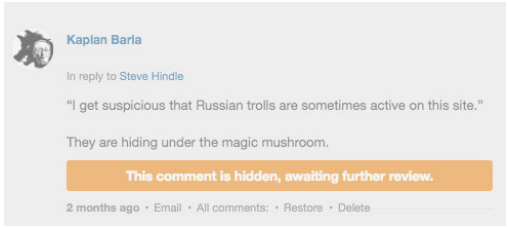


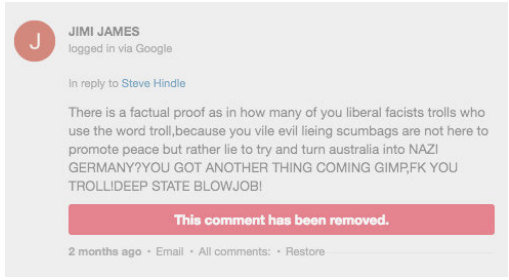


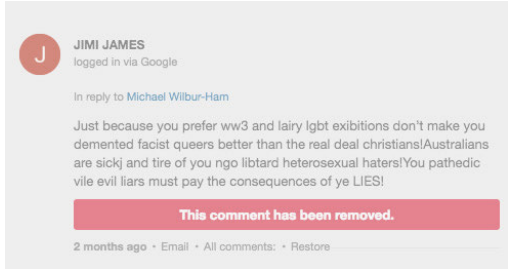


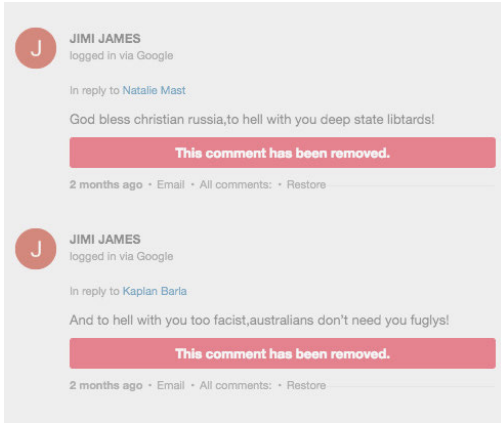


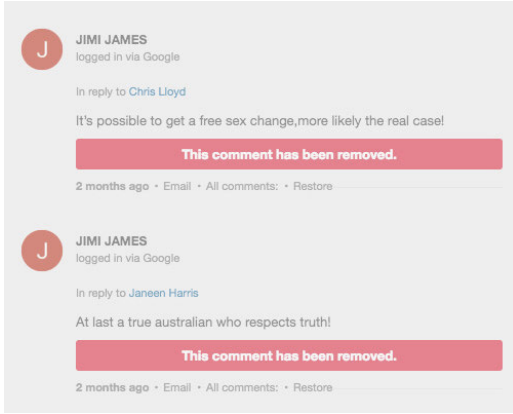


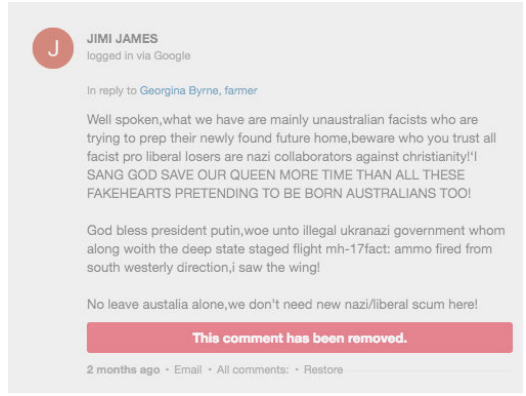


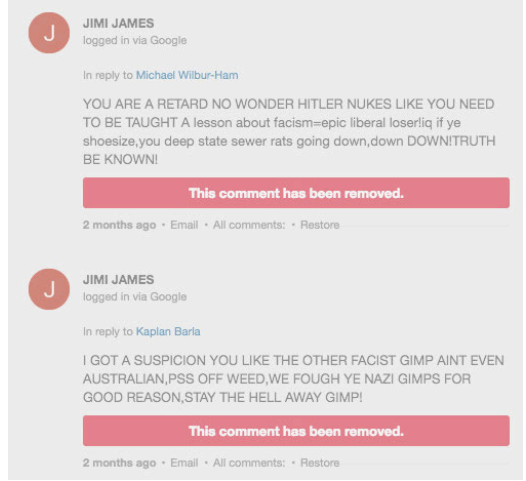



**UNSW CANBERRA CYBER**

Northcott Drive, Canberra ACT 2600

Tom Sear, UNSW Canberra Cyber

cyber.unsw.adfa.edu.au

CRICOS No. 00098G
296521638