Journal of Political Sciences & Public Affairs

Dailey, J Pol Sci Pub Aff 2017, 5:2
DOI: 10.4172/2332-0761.1000261

Perspective OMICS International

The Intelligence Club: A Comparative Look at Five Eyes

Dailey J*

Department of Security Studies and Criminal Justice, Angelo State University, Texas, USA

***Corresponding author:** Dailey J, Associate Professor, Department of Security Studies and Criminal Justice, Angelo State University, Texas, USA, Tel: 325-486-6682; E-mail: Jeffrey.dailey@angelo.edu

Received date: May 25, 2017; **Accepted date:** May 31, 2017; **Published date:** June 06, 2017

Introduction

The goal of intelligence is to evaluate data and attempt to reduce uncertainty. Successful intelligence practices try to reduce apparent ambiguity through accurate estimates and support the implementation of successful policy. The ability of intelligence communities to react to new threats and adapt and focus on relevant issues quickly and efficiently is essential for modern intelligence. A greater understanding of what comprises (or what is perceived as) an intelligence failure is important in avoiding methods that don't work; similarly, having an awareness of other states' intelligence efforts and observing different (and possibly more successful) approaches can help mitigate sedentary, too-conservative thinking. A group which has been extraordinarily successful, by any subjective or objective standard, has been the Five Eyes. Five Eyes is a surveillance arrangement comprised of the United States' National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), the Australian Signals Directorate (ASD), Canada's Communications Security Establishment (CSEC), and New Zealand's Government Communications Security Bureau (GCSB). A comparative look at Five Eyes' intelligence efforts and agencies provides an opportunity to examine what may contribute to common themes of intelligence success.

The trends discussed in this article are relatively recent, but it is important to place these in context with the general post-9/11 environment to better understand the evolution of intelligence work in the modern world. A major source of the changing strategies and practices of intelligence communities is initiated from court decisions and legislation. These direct and indirect checks on the intelligence communities attempt to place reasonable restrictions on, and provide guidance for, intelligence efforts over the long term.

Five Eyes is not a centrally organized entity but rather a coalition of affiliated independent intelligence agencies. It is the most enduring and comprehensive intelligence alliance in the world, and is uniquely situated to handle the challenges brought by globalization. Primarily a signals intelligence (SIGINT) organization, Five Eyes does not conduct covert operations, but complements each nation's respective national intelligence capability with extensive coverage on a global scale.

SIGINT, an acronym for Signals Intelligence, is one form of several types of intelligence, including HUMINT (Human Intelligence), GEOINT (Geospatial Intelligence), MASINT (Measurement and Signatures Intelligence), and OSINT (Open-Source Intelligence). As transmissions of all kinds have increased, SIGINT has become more valuable; globalization and the internet have created an environment highly conducive to its collection and analysis. SIGINT is comprised of multiple fields and practices including cryptanalysis, traffic analysis, electronic intelligence, communications intelligence, and measurement and signature intelligence.

The basis for Five Eyes was created during World War II. The United States and Britain worked closely in their SIGINT collection during the war, intercepting communications of the axis powers. This was based on a mutually beneficial relationship; Britain had cracked Germany's Enigma cipher and the United States had cracked Japan's Purple cipher. This cooperation was institutionalized with the UKUSA agreement in the 1946 post-war environment. In the context of the emerging Cold War with the Soviet Union, it was deemed necessary to continue the intelligence collaboration into peacetime as a measure to prevent potential conflict moving forward. Canada joined the alliance in 1948 and Australia and New Zealand in 1956, creating a global intelligence-sharing organization. "Over the years, the "Five Eyes" has expanded its networks and increased its partnerships with other agencies, leading to greater information-sharing on a variety of state and non-state threats to member countries[1]."

After the collapse of the Soviet Union, non-traditional threats were on the rise with attacks on US embassies in Nairobi and Dar es Salaam in August 1998, on the USS Cole in October 2000, and in New York City on September 11th 2001. The trend has not decreased in recent years. The Bali bombings targeting Australian citizens on October 12th 2002 and the London bombings on July 7th 2005 indicate the threat extends to targets other than the U.S. The mobilization of resources to prevent a direct attack on national infrastructure or citizens became a common governmental priority among the Five Eyes nations. In many ways, the challenges now facing the member intelligence communities are as great as during the Cold War.

The Five Eyes alliance allows its member nations to share the collection and analysis burden of global threats. "Precise assignments are not publicly known, but research indicates that Australia monitors South and East Asia emissions. New Zealand covers the South Pacific and Southeast Asia. The UK devotes attention to Europe and Western Russia, while the US monitors the Caribbean, China, Russia, the Middle East and Africa[2]." This collaboration has allowed its members to concentrate on distinct areas that they would not have the resources to do otherwise. "Governments across the Western world have responded and adapted, further integrating formerly separate intelligence capacities. As the technological barriers between

1 Security Intelligence Review Committee. "Checks and Balances: Reviewing Security Intelligence Through the Lens of Accountability". Annual Report 2010-2011, p: 20. http://www.sirc-csars.gc.ca/pdfs/ar_2010-2011-eng.pdf.

2 Cox J (2012) "Canada and the Five Eyes Intelligence Community". Strategic Studies working Group Papers, p: 6. http://www.cdfai.org.previewmysite.com/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf.

information systems and previously stove-piped databases continue to fall, the sharing of data has become not merely possible, but routine[3]."

United States

The American intelligence community is the largest of the Five Eyes member nations. The National Security Agency (NSA) at Ft. Meade, Maryland, is the United States' predominant SIGINT agency and therefore interacts with Five Eyes' member agencies the most. In addition to the NSA, the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) both contribute to, and draw resources from, Five Eyes member agencies. The CIA is the predominant collector of human intelligence (HUMINT), and the FBI is in charge of counter-terrorism investigations.

As a direct result of 9/11, the US intelligence community was rearranged with the intent to better align disparate agencies with new threats to national security. Different legislative acts established and defined new roles. In November 2002 Congress passed the Homeland Security Act, and the Department of Homeland Security was created to coordinate national security efforts. Due at least in part to the perception that the 9/11 attacks were an intelligence failure, Congress responded with the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA). One of the results of the IRTPA was the creation of the office of the Director of National Intelligence (DNI), as the head of the intelligence community. The post-9/11 culture demanded many changes be made to the operational methods of the intelligence community. The lack of information sharing between agencies was cited, in the 9/11 Commission Report, as a major cause of the failure to anticipate 9/11. Congress mandated the establishment of an information-sharing environment, including intelligence fusion centers that allow federal, state, local, and tribal agencies to collaborate, and data mining programs to help correct the communication breakdown between agencies [4] [1]. The goals of facilitating better communication and reducing domestic attacks are still considered high priorities. "Counterterrorism programs employ one in four members of the intelligence workforce and account for one-third of the intelligence program's spending[5]."

One of the most comprehensive steps taken to increase information sharing and reduce the risk of terrorist attacks is through the use of Suspicious Activity Reports (SARs). SARs contain information about criminal activity that could reveal pre-operative planning for terror attacks. "The Nationwide SAR Initiative (NSI) is an effort to have most federal, state, local, and tribal law enforcement organizations participate in a standardized, integrated approach to gathering, documenting, processing, and analyzing terrorism-related SARs[6]."

Some NSA programs have come under scrutiny as members of Congress and the public have raised questions about the constitutionality of some of its actions. The two programs that arguably have been the most controversial are the NSA's bulk collection of telephone metadata and its interception of internet-based communications between individuals.

The ongoing debate between individual privacy and national security goes back many years, to a relevant Supreme Court case in 1967, another in 1979, and a congressional Act in 1978. Katz vs. United States, 389 U.S. 347 (1967), involved suspected interstate gambling. Believing that Katz was a bookie taking bets from gamblers in other states, Federal agents attached a listening device to the outside of a public telephone booth, without a warrant, in order to acquire evidence to present at trial. The agents believed that since the phone booth Katz was using was public, no warrant was required. Based on the suspect's part of the recorded conversations, Katz was convicted of the transmission of illegal wagering information. Katz appealed, arguing that the recordings should not have been allowed into court, since they were acquired without a warrant. The Court of Appeals rejected his argument, based on the lack of a physical intrusion into the telephone booth. The Supreme Court granted certiorari to determine whether the Fourth Amendment protection against unreasonable searches and seizures required the police to obtain a warrant in order to wiretap a public phone booth. In a landmark decision, the Court said that the Fourth Amendment applied to "persons," not "places," and that Katz had an "expectation of privacy" which extended to a public phone booth[7].

The Smith case in 1979 was similar to Katz in that it also involved a lack of a search warrant, and an expectation of privacy (Smith vs. Maryland, 442 U.S. 735 (1979)). Patricia McDonough was robbed in Baltimore, Maryland, in March 1976. She observed a 1975 Chevrolet Monte Carlo driving away, and believed the driver was the person who robbed her. She began receiving threatening phone calls a few days later, asking that she stand on her porch at a certain time. From there, she observed what she believed was the same car, driving by. The police observed the same car on March 16, in her neighborhood, and ran the plates. The car belonged to a Michael Lee Smith. The police contacted the phone company and asked that a pen register be attached to Smith's home phone, to record dialed numbers. A day later, on March 17th, the register recorded a call from Smith's home telephone to McDonough's telephone. The police then obtained a search warrant to search his house and discovered a phone book with the corner turned down on a page with McDonough's number. He was arrested, placed in a lineup, and identified as the robber by McDonough. Because the information supplied by the pen register was obtained without a warrant, Smith filed a motion to suppress, which was denied by the trial court. Smith was convicted, and appealed. The Maryland Court of Appeals affirmed his conviction, holding there was no expectation of privacy to cover the numbers dialed into a telephone system, and no Fourth Amendment violation. The Supreme Court, in a 5-3 majority, held that a reasonable expectation of privacy does not apply to the dialed

[3] Security Intelligence Review Committee. "Bridging the Gap: Recalibrating the Machinery of Security Intelligence and Intelligence Review". Annual Report 2012-2013, p: 10. http://www.sirc-csars.gc.ca/pdfs/ar_2012-2013-eng.pdf.

[4] Bjelopera JP (2011) "Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress". Congressional Research Service. PDF p: 2. http://fpc.state.gov/documents/organization/166837.pdf.

[5] Gellman B, Miller G (2013). "Black budget' summary details U.S. spy network's successes, failures and objectives". The Washington Post. https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html.

[6] Bjelopera "Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative". PDF p: 2.

[7] Edward CL, Nolan A, Richard M. Thompson II (2014) "Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments". Congressional Research Service, p: 5. http://fpc.state.gov/documents/organization/225113.pdf.

numbers recorded by a pen register because those numbers are used in the regular business of the phone company[8]. The Court argued that Fourth Amendment protection does not apply to information voluntarily given to third parties, including the telephone numbers regularly provided to phone companies by their customers.

The 1978 Foreign Intelligence Surveillance Act (FISA) authorized the United States government to conduct surveillance on non-U.S. citizens outside the continental United States, as well as citizens suspected of working for a foreign government. FISA was a direct result of congressional committees investigating CIA and FBI surveillance activities ostensibly done in the name of national security. The 1978 FISA legislation sets out procedures for physical and electronic surveillance of persons suspected of working for foreign nations, including U.S. citizens, and non-U.S. citizens outside the United States. The 1978 legislation also established the Foreign Intelligence Surveillance Court (FISC), a special Federal court which holds nonpublic sessions to consider granting search warrants under FISA.

In order to obtain a search warrant, the Department of Justice must file an application with the FISC to obtain the warrant authorizing surveillance of foreign agents. As originally written, for "foreign agents" that are U.S. persons, including U.S. citizens, the government must demonstrate probable cause to believe that the "target of the surveillance is a foreign power or agent of a foreign power," that a "significant purpose" of the surveillance is to obtain "foreign intelligence information," and that appropriate "minimization procedures" are in place[9]. FISA was amended in 2008, with the FISA Amendments Act, which empowered the FISC to authorize surveillance without a requisite showing of probable cause that the target of the surveillance is an agent of a foreign power. Subsequent to the 2008 Act, the government need only demonstrate that the surveillance targets "persons reasonably believed to be located outside the United States" and seeks "foreign intelligence information."

At some point prior to June 5, 2013, the Department of Justice applied for and received a warrant authorizing the FISC to order Verizon Business Network Services to turn over on "an ongoing daily basis" phone call details including whom calls are placed to and from, when the calls were made, and how long they lasted. This is known as metadata. It contains the pertinent information relating to the phone call, except for the content of the call itself.

"Upon public revelation of the NSA's bulk telephony metadata program, several lawsuits were filed in federal district courts challenging the constitutionality of this program under the Fourth Amendment's prohibition against unreasonable searches and seizure[10]." Two notable court cases were American Civil Liberties Union vs. Clapper (No. 13-3994 (S.D. New York December 28, 2013)), and Klayman Vs. Obama (957 F.Supp.2d (2013)), because they resulted in different rulings. In ACLU vs. Clapper it was determined that the collection of bulk data did not constitute a search based on the third-party doctrine described in Smith vs. Maryland, above, and thus did not violate the Fourth Amendment[11].

The Klayman case, although facially similar to ACLU vs. Clapper (NSA had asked the FISC to order phone companies to turn over client data regarding phone calls), had an entirely different ruling. Federal Judge Richard J. Leon decided on December 16, 2013, that the collection of telephone metadata likely violated the United States Constitution. He also ruled that the 1979 Smith vs. Maryland case cited by the judges in the ACLU vs. Clapper case did not apply to the NSA program, as they had argued, and that the search was not reasonable under the Fourth Amendment[12].

Constitutional challenges to the NSA's acquisition of internet communications have appeared from private citizens involved in court cases who were alerted that their cases were derived from information gathered under Section 702 of the Foreign Intelligence Surveillance Act (FISA). Clapper vs. Amnesty International (133 S.Ct. 1138 (2013)) was a suit brought to challenge the joint authorization procedure for surveillance of non-US persons abroad on the grounds of the Fourth Amendment's prohibition against unreasonable searches. The US Supreme Court determined that the plaintiffs had not suffered a sufficiently concrete injury to have the legal standing to challenge Title VII[13]. An important distinction between the acquisition of internet communications and the collection of bulk telephone metadata is that internet communications include the content of the messages while the bulk telephone data does not.

These cases are related to how SIGINT is currently collected in the United States. If the NSA is rendered unable to utilize its usual methods of collection, it may be unable to meet the demands of national security placed upon it by Congress and the American public. These challenges affect not only the United States directly, but Five Eyes as a whole.

Overall, to this point, the United States has been arguably successful in its intelligence efforts. "The death of Osama bin Laden, and the series of US drone attacks against senior leaders in the Federally Administered Tribal Areas of Pakistan (FATA), has weakened Al-Qaeda Core's capability[14]." On the domestic counter-terrorism front, the US has successfully foiled 39 terrorist plots in the period between September 2001 and May 2011[15]. The 'Black Budget' for 2013 leaked by Edward Snowden revealed how the US intelligence community was prioritizing its resources and provided a brief summary of the numbers of intelligence undertakings. "The document describes a constellation of spy agencies that track millions of surveillance targets and carry out operations that include hundreds of lethal strikes. They are organized

8 Ibid. Page 7.

9 Ibid.

10 Ibid. p: 14.

11 Rifkind M (2012) Intelligence and Security Committee of Parliament. Annual Report 2011-2012, p: 20. http://isc.independent.gov.uk/committee-reports/annual-reports.

12 Gellman, Miller. Black budget.

13 Greg Fyffe (2011) "The Canadian Intelligence Community After 9/11", Spring. Journal of Military and Strategic Studies 13(3): 4.https://www.ciaonet.org/attachments/19088/uploads.

14 Security Intelligence Review Committee. "Meeting the Challenge: Moving Forward In a Changing Landscape". Annual Report 2011-2012. p: 11. http://www.sirc-csars.gc.ca/pdfs/ar_2011-2012-eng.pdf.

15 "Canada's electronic spy agency stops sharing some metadata with partners". CBC News. January 28, 2016. http://www.cbc.ca/news/politics/spy-canada-electronic-metadata-1.3423565.

around five priorities: combating terrorism, stopping the spread of nuclear and other unconventional weapons, warning U.S. leaders about critical events overseas, defending against foreign espionage, and conducting cyber-operations[16]."

Canada

Canada's intelligence community is much smaller than that of the United States. However, Canada's professionalism and unique geography continue to make it an ally as valuable now as during the Cold War. The Communications Security Establishment (CSE) is Canada's SIGINT agency; the Canadian Security Intelligence Service (CSIS) is the HUMINT agency.

Canada's intelligence community suffered badly during the 'peace dividend', the reduction in funding for intelligence and military purposes in the decade following the end of the Cold War. After the threat of international terrorism became apparent, Canada quickly returned to Cold War-levels of funding to counter the danger. A common thread throughout Five Eyes, Canada's spending increased dramatically in the post 9/11 environment. "From 1999-2000 to 2008-09 the budget of CSIS rose from $179 million to $430 million. Staffing climbed from 2,061 to 2,910 in that period[17]." International Counter Terrorism (ICT) efforts have increased dramatically as well with the implementation of various plans directed expressly for this area of focus. One of the noticeable components to aviation security in Canada is the Passenger Protection Program (PPP). It incorporates the "no-fly list" implemented in the Aeronautics Act, allowing airports to cross reference passengers with the Specified Persons List to deny boarding if it is believed they pose an "immediate threat"[18].

Canada has recently declared its intent to overhaul its oversight process for intelligence. In January 2016 the CSE temporarily halted its metadata information sharing with other Five Eyes members after realizing the information had not been minimized correctly[19]. Minimization is the process of rendering information of nationals unidentifiable prior to sharing the metadata information. Canadian intelligence organizations have separate independent oversight agencies, and there is currently no agency which oversees the Canadian security and intelligence community as a whole, and no Parliamentary oversight. "There is no cabinet committee dedicated exclusively to S&I [Security and Intelligence] questions; there is no parliamentary oversight mechanism which can consistently monitor the community; and, the bureaucratic oversight has been built through agency-specific mechanisms[20]." Potential reforms include greater interagency cooperation among review committees and increased resource capacity. Canada is currently in the process of a national security review to determine the appropriate plan moving forward. Possible options include modifying the Security Intelligence Review Committee or implementing a British-style parliamentary oversight process.

Canada has had success in its interagency coordination efforts. The "Toronto 18" investigation is one example of the combination of utilizing SIGINT from internet communications and HUMINT from the penetration of the group. "As a result, threat-related online activities have moved to the forefront of many national security investigations. This medium has come to play an important operational role in CSIS investigations: for example, key targets of the "Toronto 18" group were initially detected through the monitoring of material posted online[21]." "Recent successful human source operations reinforce this point: human sources' penetration of, and reporting on, the Toronto 18 terrorist cell, for example, were instrumental in the successful prosecution of the main conspirators[22]." The functions of HUMINT and SIGINT collection, although historically detached from one another, are changing as intelligence disciplines are merging to better address the modern technologically complex environment. This was represented in Canada as the CSE headquarters was moved alongside CSIS headquarters in 2014[23].

The focus of Canada's intelligence agencies is much more internal than the United States. Canadian intelligence works independently at the domestic level, gathering information relevant to its national interests and maintaining a robust ICT culture. At the international level, Canadian intelligence focuses on its foreign relationships and policies. "The effectiveness of an intelligence community must be assessed in many dimensions. Absolute level of resources is very important, but so is the relationship with allies. Canada exchanges information and assessments within the Five Eyes community, and there is extensive operational interaction[24]."

Australia

Like Canada, Australia does not have an intelligence culture at the same level as the US. Due to its relative geographic isolation, it maintains a stronger intelligence community than Canada. Australia has been a large contributor toward the continued collaboration of intelligence among Five Eyes. Besides Five Eyes; Australia, New Zealand, and the United States are bound by the ANZUS collective security agreement established in 1951, further integrating defense intelligence. "Access to partners' intelligence is a huge multiplier to the capabilities and effectiveness of our intelligence agencies[25]." Australia's

16 Fyffe, p: 14.

17 SIRC (2010-2011). p: 12.

18 Ibid. Page 23.

19 SIRC (2012-2013). p: 16.

20 Fyffe, p: 3.

21 Robert CAO, Dr. Rufus B (2011) Independent Review of the Intelligence Community Report, p: 17. https://www.dpmc.gov.au/sites/default/files/publications/2011-iric-report.pdf.

22 Waddell AP (2015) "Cooperation and Integration among Australia's National Security Community". Studies in Intelligence. 59(3): 28. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-3/pdfs/Cooperation-and-Integration-Among-Australias-NSC.pdf.

23 Davies A (2015). "Australia's intel cooperation with Iran: eyes wide shut?" Australian Strategic Policy Institute. http://www.aspistrategist.org.au/au-intel-cooperation-with-iran-eyes-wide-shut/.

24 Kitteridge R(2013) . Review of Compliance at the Government Security Communications Bureau, p: 12. http://www.gcsb.govt.nz/assets/GCSB-Compliance-Review/Review-of-Compliance.pdf.

25 Ibid.

primary SIGINT agency is the Australian Signals Directorate (ASD), the Australian Secret Intelligence Service (ASIS) is the foremost HUMINT agency, and the Australian Security Intelligence Organization (ASIO) is the country's main security, counter-intelligence and counter-terrorism agency.

Australia began transitioning out of the 'peace dividend' era of the 1990's earlier than its Five Eyes' allies, in anticipation of the 2000 Sydney Olympic Games. The events of 9/11 and the Bali bombings on October 12th 2002 that claimed 89 Australian lives further reinforced the resolve of Australia to safeguard the nation against this threat. "The number of agencies encompassed in the NSC has increased and their allocated budgets have increased accordingly; for example, ASIO's budget increased from $69 million in 2001 to $430 million in 2010, a rise in keeping with the increasing level of complex threat [26] [2]."

Australia is an excellent case study of how interactions among Five Eyes nations are changing to meet respective national problems. While maintaining strong ties to Five Eyes, Australia has also pursued its own objectives that do not entirely coincide with other members of the Five Eyes alliance. In October of 2014 Australia made the beginnings of an arrangement to share intelligence with Iran pertaining to the war against ISIS[27]. Australia's interest is influenced by the desire to track Australians that have traveled to the Middle East to join ISIS, potentially a great threat to the domestic safety of Australia. There have been critics of this policy pointing out that Iran has been a poor intelligence partner in the past and arguing the Iranian information poses the risk of falsified intelligence meant to deceive. However, it is likely that Australia is trading just enough intelligence to get what it wants, and examining the intelligence given to it with a critical eye.

One point of contrast between the US and Australia in how they conduct their counterterrorism operations is the specified roles each country's lead agencies play. America's primary counter-terrorism agency is the FBI, predominantly a law enforcement agency. Australia's lead counter-terrorism agency is the ASIO which by national law cannot conduct law enforcement operations; it must collaborate with the Australian Federal Police for domestic operations.

New Zealand

"The core New Zealand Intelligence Community (NZIC) comprises GCSB, the New Zealand Security Intelligence Service (NZSIS), and parts of the Department of the Prime Minister and Cabinet (DPMC)[28]." The GCSB, Government Communications Security Bureau, has two main functions: information assurance and obtaining foreign signals intelligence. The NZSIS is New Zealand's HUMINT collection agency. The parts of the DPMC that work alongside the rest of the NZIC are the National Assessments Bureau (NAB) which collates and analyzes information on foreign countries, and the Officials Committee for Domestic and External Security Co-ordination (ODESC) which coordinates all agencies in security situations. "Real change has been evident in the way that the community operates as a collective, resulting in a better use of scarce resources in the interests of New Zealand's national security[29]."

The most impactful event for New Zealand's intelligence community in the last several years was the arrest of Kim Dotcom and the subsequent Review of Compliance by Rebecca Kitteridge. In January 2012 New Zealand law enforcement entered Kim Dotcom's property searching for and seizing alleged evidence of US copyright infringements. Dotcom was arrested and his property seized under the auspices of the Mutual Legal Assistance Treaty between New Zealand and the US. What makes this pertinent to the discussion of New Zealand's intelligence efforts is the interaction between the GCSB and the New Zealand police. The GCSB supported the police by intercepting Dotcom's communications and tracking his movements. However, this violated GCSB Act article 14: '[n]either the Director, [n]or an employee of neither the bureau, nor a person acting on behalf of the bureau may authorize or take any action for the purpose of intercepting the communications of a person who is a New Zealand citizen or a permanent resident[30].'

This failure of roles was partly due to the confusion over the definition of national security. The subsequent compliance audit was to ensure proper safeguards were in place to protect New Zealanders and confirm the GCSB was following its protocols in a lawful manner. "It should be noted that my review was focused on GCSB's operations and whether there are systems in place to ensure the lawfulness of those operations under relevant New Zealand and international law [31][32]Kitteridge report recommendations, GCSB now has a comprehensive framework of processes, tools and structures in place to support the effective management of compliance obligations[33]."

The GCSB has placed great emphasis on cyber security moving forward. This is a natural extension of capabilities for New Zealand's primary SIGINT agency. "GCSB plays a vital role in New Zealand's security by obtaining, providing and protecting sensitive information[34]." New Zealand's most common cyber-attacks target individuals rather than organizations or infrastructures; these are usually in the form of an e-mail that contains malicious attachments or links. A part of GCSB's cyber security work is the CORTEX project, which protects critical infrastructure organizations. "The organizations receiving CORTEX protections include government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure[35]." GCSBs National Cyber

26 Rogers D (2015.) "Extraditing Kim Dotcom: A case for reforming New Zealand's intelligence community?" Kōtuitui. New Zealand Journal of Social Sciences 10 (1). http://www.tandfonline.com/doi/full/10.1080/1177083X.2014.992791.

27 Kitteridge. Review of Compliance, p: 13.

28 Government Communications Security Bureau. Annual Report For The Year Ended 30 June 2015. p: 12. http://www.gcsb.govt.nz/assets/GCSB-Annual-Reports/GCSB-Annual-Report-2015.pdf.

29 Ibid.

30 Kitteridge. Review of Compliance, p: 11.

31 "Cyber Security: GCSB's contribution to combatting cyber threats". The New Zealand Intelligence and Security Bill 2016. Department of the Prime Minister and Cabinet. Case Study No. 4. https://www.dpmc.govt.nz/sites/all/files/NZIS%20Bill%20Case%20study%204%20-%20Cyber%20security%20-%20WEB%20FINAL.pdf.

32 Ibid.

33 GCSB. Annual Report 2015. p: 11.

34 Rifkind. ISC. Annual Report 2011-2012, p: 43.

Security Center provides service for 17 different organizations and has logged multiple cyber intrusions. In the 12 months ending on June 30th 2015 there were 190 cyber-attacks reported, compared to 316 in the 12 months ending on April 1st 2016 [36].

New Zealand's small size and geographically limited area makes wide-ranging SIGINT efforts difficult. Because of Five Eyes, New Zealand is able to have a much broader picture of global intelligence than it would otherwise. "It is not possible for an organization the size of GCSB to collect foreign intelligence on all matters relevant to New Zealand's interests. However, through long-standing relationships with our Five Eyes partners, we can draw on greater support, technology and intelligence than would otherwise be available to us[37]."

United Kingdom

The United Kingdom's primary SIGINT agency is the Government Communications Headquarters (GCHQ); the main HUMINT agency for threats outside the country is the Secret Intelligence Service (SIS or MI6), and its domestic security intelligence service is the Security Service (MI5). The UK's intelligence agencies are some of the oldest and most respected; they have shown a great deal of innovation in collecting and analyzing information regardless of budget conditions. "It would be difficult, if not impossible, for our Agencies to confront such threats if they worked in isolation; to protect our national security they depend on intelligence shared with us by our foreign partners[38]."

The coordinated terrorist attacks on July 7th 2005 were a shock to Britain. It had become clear shortly after the 9/11 attacks in America that the radical Islamist threat was not singularly focused on the US but rather the West and its values. The attacks in 2005 in England killed 56 and injured 784. At the inquest, the coroner concluded that "the police and the Security Service could not reasonably have prevented the 7/7 bombings given the resources at their disposal and the high priority threats they were facing mirrors the Committee's own conclusions in its 2009 report[39]." After this the UK placed much more emphasis on counter-terrorism planning and funding. "ICT is also the highest priority for GCHQ and SIS, accounting for around a third of the effort of both[40]." The prioritization of ICT efforts has been true for all of the UKs intelligence agencies, along with proportionate increases in funding. "After the terrorist attacks in London on 7 July 2005, the Government accelerated the planned funding increases. As a result the SIA has increased from approximately £800 m to £2 bn (in cash terms) over the last decade[41]." Since these modifications were made Britain has had definite success at identifying and preventing terrorist attacks at home. "It is clear that coverage of terrorist groups is by no means comprehensive. Resources need to be shifted to target the most pressing issues. Nevertheless, they have had notable successes: nine men were jailed in February 2012 for plotting to bomb the London Stock Exchange and establish a terrorist training camp[42]." In an SIS report to the Intelligence and Security Committee of Parliament it stated that although the ICT threat is constantly evolving they were able to stay up to date to the scale of the challenge. With their global coverage and network of foreign liaison partnerships, they regard the threat as "broadly contained"[43] [3].

In addition to the threat of terrorism originating from the Middle East, Great Britain continues to put resources into Northern Ireland counter-terrorism efforts to prevent attacks from the Irish Republican Army. In 2009 there were 22 attacks on critical infrastructure targets by the IRA; in 2010 there were 40, and in 2011 there were 26. "The Committee was told that the reduction [in the number of IRA attacks] was the result of intense activity by the police in Northern Ireland, who had made over 200 arrests for terrorism-related offences[44]."

Organizational changes related to national security and intelligence have become commonplace for the UK over the last several years. In 2010 the National Security Council (NSC) was established to consider matters related to national defense, foreign policy, foreign relations, and intelligence coordination. The 2010-2011 annual report by the Intelligence and Security Committee of Parliament provided several quotes by the leaders of the UKs intelligence agencies regarding the NSC. The chief of the SIS stated that the NSC was "a valuable step forward" and that a weekly meeting "enabled senior Ministers to have a fuller sense of the intelligence underpinning of the issues that they are addressing[45]." The Director of the GCHQ stated that "The quality of the debate and the exploration is first class. The chairmanship is robust but accessible[46]." The Director General of the Security Service stated that the NSC provided "greater clarity on priorities and policy in the national security area than was available from previous arrangements." Other legislation that affects UK intelligence practices include the Investigatory Powers Bill, which was introduced to the House of Commons on March 1st 2016 and is currently under consideration. The Investigatory Powers Bill is meant to clarify Britain's role in intercepting communications data by providing new powers for the intelligence community and law enforcement while introducing an Investigatory Powers Commission to ensure compliance.

35 Sir Rifkind M (2011). Intelligence and Security Committee of Parliament, Annual Report p: 6. http://isc.independent.gov.uk/committee-reports/annual-reports.

36 Rifkind. ISC. Annual Report 2011-2012, p: 23.

37 Rifkind. ISC. Annual Report 2010-2011, p: 12.

38 Rifkind (2012) ISC. Annual Report 2011-2012, p: 21.

39 Rifkind (2011) ISC, Annual Report 2010-2011, p: 33.

40 Rifkind (2012) ISC, Annual Report 2011-2012, p: 28.

41 Rifkind (2013) Intelligence and Security Committee of Parliament. Annual Report 2012-2013, p: 11. http://isc.independent.gov.uk/committee-reports/annual-reports.

42 Comey JB (2015). Oversight of the Federal Bureau of Investigation. Statement Before the House Judiciary Committee. https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-7.

43 Phil Helsel. "Australia Christmas Terror Plot Foiled, Police Say". NBC News. http://www.nbcnews.com/storyline/isis-terror/australia-christmas-terror-plot-foiled-police-say-n699381.

44 2016 Public Report on the Terrorist Threat to Canada. Cat. No. pS4-200/2016 E. Pdf. http://www.2016-pblc-rpr-trrrst-thrt-en.

45 Kredo A. "ISIS Terrorists Infiltrating Canada, Suspected of Plotting Attacks." http://freebeacon.com/national-security/isis-terrorists-infiltrating-canada-suspected-plotting-attacks/.

46 Ibid.

Future of Five Eyes

There exist many challenges ahead for the alliance. These include the increased independence of terrorist organizations, international crime, and cyber-attacks. "There is no doubt that the more sophisticated people in Al-Qaeda recognize that [organized] groups are, in some ways, a thing of the past; and that encouraging lone acts of terror is exactly the way forward [47]." Friction between the members of Five Eyes has happened in the past and each nation has the potential to disrupt the alliance. Most importantly, Five Eyes and its component nations must find equilibrium between utilizing methods to enhance productivity of intelligence gathering and respecting citizens' rights to privacy.

Modern non-state entities pose a common threat to the national security and interests of the Five Eyes nations. Multinational organizations such as terrorist cells and organized crime cannot be minimized through unilateral action; extraterritorial borders and laws restrict the preventative measures that could be employed. International cooperation is needed to address these issues. Five Eyes nations are adapting to these challenges by implementing new roles to handle complex issues. One such role is the Five Eyes Law Enforcement Group (FELEG), comprised of law enforcement and intelligence agency subject matter experts from the FBI, National Crime Agency, Royal Canadian Mounted Police, Australian Federal Police, and New Zealand Police. "The FELEG coordinates government international responses to global organized crime, money laundering, and cyber-crime. Key goals of the FELEG are to improve the ability of partners to share intelligence and conduct joint law enforcement operations, while ensuring that they leverage one another's capabilities and benefit from shared learning and best practices[48]."

The danger to individual member nations from terrorist groups has not diminished in recent years. Attacks directly or indirectly attributed to ISIS have occurred in each country. For example, in Australia, Victoria Police Chief Commissioner Graham Ashton reported during a news conference on December 23rd, 2016, that the police had foiled a plan to bomb parts of Melbourne on Christmas Day in an attack inspired by ISIS. Seven people were arrested in raids in northwest Melbourne in a plot involving explosives and possibly knives or guns, against civilian targets in the heart of the city of 4 million, including areas near Federation Square, Flinders Street Station, and St. Paul's Cathedral. According to Ashton, police believe that the suspects were "self-radicalized but certainly inspired by ISIS and ISIS propaganda and have been persons of interest for Victoria police and intelligence agencies now for some period of time" but interest accelerated and an investigation was launched. The terrorism level in Australia was raised to "probable" in 2014 due to threats posed by ISIS. The office of the Australian Prime Minister reports that since that point, 57 people have been charged in 27 counter-terrorism operations in the country. During 2014 and 2015, Australia experienced three attacks-two targeting police officers in Melbourne and Sydney (September 2014, October 2015) and another targeting civilians in Sydney (December 2014).

In Canada, as in other countries, the biggest threat appears to originate with nationals who travel abroad to join terrorist groups and then return to their home country to commit terrorist acts. The government in Canada is warning citizens that "at least" 180 individuals have left the country to join groups like ISIS and it is currently tracking 60 who have returned to Canada. Individuals who have traveled abroad to communicate with terrorist groups and then make their way back to North America raise legitimate concerns that ISIS and its affiliates are planning attacks on the continent. According to the Canadian government report, "Since the beginning of the Syrian conflict in 2011, more than 36,500 extremist travelers from over 100 countries, including at least 6,600 individuals from Western countries, have travelled to Syria." Some of those individuals returned to North America: "about 60 extremist travelers had returned to Canada," according to the report. The specific intentions of those individuals are unknown. "The experiences and intentions of these individuals vary. They may have skills, experience and relationships developed abroad that could be used to recruit or inspire individuals in Canada." "Since 2002, 20 individuals have been convicted of terrorism offences under the Criminal Code. Another 21 have been charged with terrorism-related offences (including 16 since January 2015) and are either awaiting trial or have warrants outstanding for their arrest."

The United States of America and Western Europe experienced multiple attacks attributed to ISIS in 2015, including the attacks on police officers in Boston, in June, 2015, military facilities in Chattanooga, Tennessee, in July, and an attack during an office party in San Bernardino, California, in December of 2015. The new forms of terrorism cross all the borders. Radical terrorists hatch plots without ever contacting known terrorists, which limits our ability to monitor their movements, or plans. In the United States, the expression of radical views is protected by the Constitution. The ongoing and constant challenge is to try to identify the triggers for violence and attempt to intervene at the right moment to prevent it.

In spite of our best efforts to prevent them, terrorist incidents continue to occur. In June 2016, 49 people were killed and 53 injured when a gunman, who may have been inspired by ISIS propaganda, opened fire at an Orlando, Florida night club. In July, 85 people were killed and hundreds more were injured when an attacker drove a truck through a crowd in Nice. There have been other attacks in Western Europe as well, for example, in Brussels, Belgium and in Rouen, France. In Turkey this past June, suicide bombers believed to be affiliated with ISIS struck Istanbul's international airport, killing 45 and injuring over 200.

ISIS-related activity in the United States has been unprecedented. During the fall of 2015, US authorities reported approximately 250 American citizens who had either traveled to or attempted travel to Syria/Iraq and/or join the Islamic State in Iraq and Syria (ISIS). In addition, they also reported 900 active investigations against ISIS sympathizers. Seventy-one individuals have been charged with ISIS-related activity inside the United States since March 2014, and fifty-six in 2015 alone.

In London on March 22, 2017, a British man, Khalid Masood, with ties to ISIS, carried out the deadliest terrorist attack on English soil in 12 years. According to British Prime Minister Theresa May, the attacker was linked to violent Islamic extremism. Four people were killed, including an American tourist and a British woman of Spanish origin, when Masood rammed a rental car into a group of tourists on Westminster Bridge in London. Masood then stabbed a British police officer to death. The Prime Minister said that police, security forces and intelligence agencies have successfully thwarted 13 separate terrorist plots in Great Britain since 2013. She said the current threat

47 Public Report on the Terrorist Threat to Canada (2016) Cat. No. pS4-200/2016 E. Pdf. http://www.2016-pblc-rpr-trrrst-thrt-en.

48 Ibid.

level (severe) would not be raised to Critical because "there was no specific intelligence that an attack was imminent."

After the negative publicity surrounding the telephone metadata collection and other mass surveillance programs there has been a significant push to have Five Eyes dismantled. Intelligence oversight and audits are an integral part of the intelligence process as well as the protection of individual privacy. The tension between the collection of information related to national security and individual privacy rights of the individual in liberal democratic states has increased markedly since 9/11. The regular review of intelligence services ensures that the fundamental rights of citizens are respected while threats to national security are minimized.

References

1. http://fpc.state.gov/documents/organization/166837.pdf.
2. Rogers D (2015) Extraditing Kim Dotcom: a case for reforming New Zealand's intelligence community? Kōtuitui: New Zealand Journal of Social Sciences Online 10: 46-57.
3. Phil H (2016) Australia Christmas Terror Plot Foiled, Police Say. NBC News.

This article was originally published in a special issue, entitled: **"Special Homeland Security Issue",** Edited by Anthony N. Celso