TML WEEKLY
INFORMATION PROJECT

February 24, 2018 - No. 7

Supplement

Talk About Cyber Attacks and "Weaponization" of Social Media

• NATO on Social Media -- The Threat to Liberal Democracy
• Making Foreign Influence a New Domestic Crime -- The Australian Example

---

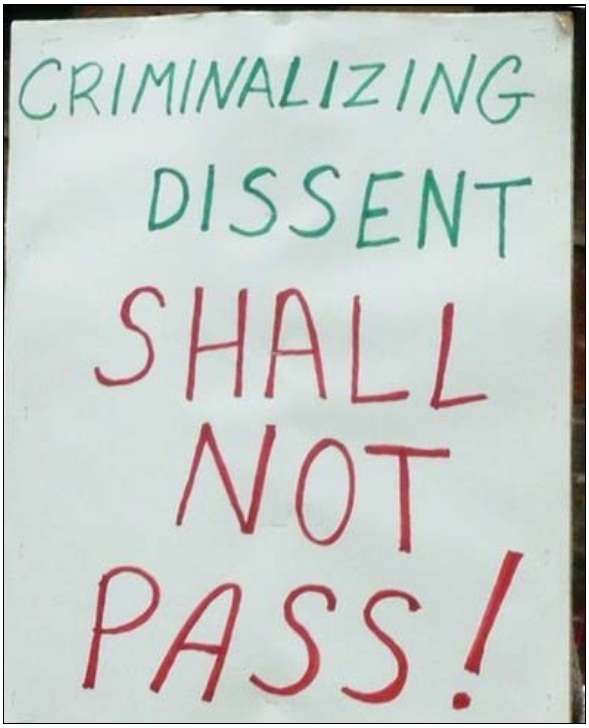
Talk About Cyber Attacks and "Weaponization" of Social Media

NATO on Social Media -- The Threat to Liberal Democracy

It has become increasingly clear that the U.S.-led NATO aggressive alliance is directing the anti-democratic measures being taken in Canada and other NATO member countries to criminalize conscience and speech, in the name of defending democracy and national security. The assault on conscience and speech targets speech that opposes NATO and is critical of the political and electoral systems in the NATO member states. Combined, this represents a broad assault on freedom of conscience and speech and the struggles of the peoples to affirm their rights and for empowerment.

In October 2017, NATO's Parliamentary Assembly (NATO PA) issued a report entitled "The Social Media Revolution: Political and Security Implications." It was produced by the Sub-Committee on Democratic Governance with Canadian Senator Jane Cordy serving as rapporteur. The Sub-Committee on Democratic Governance works under the Committee on the Civil Dimension of

Security. The aim of the report is stated as being "to raise awareness and launch a discussion among members on this emergent theme and to offer some initial thoughts on ways to counter the malicious use of social media."



The introduction to the report is about the rise in social media use. It states that the "dramatic transformation of information and communication technology" along with growing use of social media is "changing the way we look at security ... and demands innovative responses." Twitter and Facebook, the report says, "amplify the voices of and decrease the cost for people to connect more intimately and to communicate and organize among themselves and with their governments." The possibility of anonymous use of social media, "can embolden those who propagate hate speech as equally as those fighting against authoritarian regimes without fear of reprisal."

It speaks of the resulting "weaponization" of social media, summed up as follows: Social media "provides new opportunities for those who seek to disrupt the liberal democratic world order by using the intrinsic openness of the cyber domain." Social media is used by "terrorist organizations as a recruiting and propaganda tool." Social media is "exploited by states that seek to influence and undermine liberal democracies, their government institutions and their social fabric -- at times, to great effect."

The rest of the report is broken into the following sections:

1) Social Media and Democratic Governance;
2) The 'Weaponization' of Social Media, a) Daesh and Social Media, and b) Social Media as a Foreign Policy Tool: The Case of Russia;
3) Responses to Social Media's Security Challenges; and
4) Conclusions.

Merging the Threat of Terrorism with "Foreign Influence"

Following the issuance of this report, NATO countries such as Canada have started to speak of the terrorist threat and the far from proven threat of "foreign influence in elections" as one and the same, the former causing "loss of life" and the latter "threaten[ing] to weaken and divide the Western world." By sleight of hand, the threat of terrorism and measures to counter it are merged with opposition to NATO, which is synonymous with opposition to war and to the elitist system called liberal democracy. The same security forces tasked with combating terrorism are being "re-tasked" to identify what are deemed to be "foreign influenced" opinions about NATO and democracy. A thought-control police has been empowered to attack the right to conscience of all human beings, with freedom of speech during and between elections the first casualty.

Social-Media Charged with Censorship Duties

Based on this faulty self-serving argument that opposition to NATO and a discredited electoral

process are foreign-inspired and pose a danger to national security, the implementation of a system of censorship is being placed in the hands of social media mega-giants such as Facebook and Google. This places censorship outside of the public domain, beyond the reach of public mechanisms that are supposed to provide recourse to such an abuse of police powers. The "terms and conditions" of social media platforms define what they can or cannot do in terms of denial of service, removal of postings and blogs, etc. You either accept them or are deprived of their use.

On November 1, 2017, the social media monopolies Twitter, Facebook and Google testified in front of the U.S. House Intelligence Committee on allegations of the use of social media by "Russians" to interfere in the U.S. elections.

The day prior, October 31, 2017, the Judiciary Crime and Terrorism Subcommittee held hearings on "ways to combat and reduce the amount of Russian propaganda and extremist content online," at which various executives of these social media monopolies also testified.

During these two hearings, members of the Committee released what it claimed was evidence of Russian-bought social media ads used during the U.S. presidential election. Many of the ads were provided by Facebook itself earlier in the year.

Examples of so-called Russian-bought Facebook ads posted during the 2016 U.S. presidential election campaign (click to enlarge).

Ads included Black Lives Matter posts, as well as many others, both for or against Trump and Clinton, in an effort to show that these Russian-bought ads were aimed at the election itself and not simply electing Trump, as has been alleged.

Of note, throughout this whole process, the power of Facebook and those who use it to influence and disinform the population was on full display, no doubt a promotional coup to sell even more ads and consumer information.

Also of note, this platform was used by Facebook to present itself as a legitimate force to police political discourse through its app and to announce a substantial increase in its hiring of people to police its users' activities.

Colin Stretch, a vice president general counsel for Facebook, told the Senate Judiciary Committee that "Today, across our safety, security, and product and community operation teams, we have about 10,000 people who are working on safety and security generally," adding "We're committed to investing more and **doubling** [*emphasis added*] that number by the end of 2018." This additional 10,000 is inclusive of the 4,000 already planned, the company said adding that some of the new hires will be contractors. What kind of contractors it does not say, although no doubt they could be former or current state agents.

This will be a significant increase as it is reported that as of June 30, 2017, the company had a total of 20,658 employees. He indicated that Facebook has thousands of people who specifically focus on what they called "terrorist content" and 150 who spend all their time removing "terrorism-related content," Stretch said.

Meanwhile it is reported that on November 1, 2017, Facebook Inc.'s third-quarter profit jumped 79 per cent on its continued dominance in online advertising.

Defence of "Western Values"

Photo of NATO's Cyber Coalition 17 military exercise in Tartu, Estonia, that ran November 27 to December 1, 2017.

In the concluding points, the NATO report states: "While the West may have invented social media, their genesis never promised that their networks or users would adopt Western values. Countering these new threats should be elevated to the top of the Euro-Atlantic community's agenda. Terrorist and other hostile uses of social media have already resulted in the loss of human life, and have threatened to weaken and divide the Western world."

It also says that when social media is used to propagate "false and disruptive stories," it "shake[s] the confidence citizens have in their institutions and leaders."

According to the report, "social media has had a profound impact on democratic institutions and political life across the globe" with "[c]itizens in general and political actors in particular hav[ing] used social media sites, such as Twitter and Facebook, to challenge the political establishment and rally voices across the political spectrum." In the U.S., it says, "over a third of new social media users regularly direct their activity to commenting on government and politics." In regards to Canada, it notes that "civic society teamed up with Google to find innovative ways to increase voter turnout" in the 2015 federal election.

To cover up that intelligence services have completely failed in their job when it comes to predicting any major event that has taken place in the last twenty years, the NATO report blames both Brexit in Britain and the Trump victory in the U.S. as evidence that "user activity on social media sites is proving to be anecdotally predictive of campaigns." For example, it claims that after Brexit, a conclusion is that "campaigners underappreciated the popularity of 'Leave' on social media and how that would translate into votes."

The report is in total denial that the manipulators of social media to launch PR campaigns against rivals in an election are the cartel political parties, which even hire foreign firms to manipulate results. The report says that social media can turn any individual into an "information actor." The "relative success of many anti-establishment parties in the Euro-Atlantic area may be attributed to skillful social media strategies. Often the most prolific political accounts are far-left and far-right anti-establishment party leaders and groups."

The conclusion drawn by NATO is that "the loudest and most engaged voices online are producing deep political change, but those calls increasingly come from polar ends of the political spectrum."

Social Media as a Foreign Policy Tool

The report then charges that Russia has "weaponised information turning media into a weapon of mass deception/distraction and a *de facto* extension of its military and diplomacy." It provides this as an excuse for NATO to also use social media for military purposes. The report quotes former Deputy Director of the U.S. National Security Agency John Chris Inglis saying that Russia is 10 years ahead of the United States "in using social media for information operations" and is using this superiority to "play a great power game without a great power's resources."

The objectives of Russia's information war, the report says, are to "monopolize the information space within Russia in order to 'neutralize' external information activities targeting Russians" and "to project Russia's interest abroad." It says, "Moscow skillfully exploits the pluralistic nature of the media in Western societies and the fact that Western governments have little control over the media in their countries."

The report suggests that Russian President Putin's strategy is more effective than that of the former Soviet Union because "Putin's Russia does not project a clear ideology; its propaganda machine does not have to convince audiences that Russia's model is superior." Instead, it says "the goal is to demoralize and divide Western societies and to establish moral equivalence between Russia and the West by promoting the notion of Western hypocrisy. For instance, the Kremlin's response to extensive Western reporting that Russia's parliamentary and presidential elections were rigged was to suggest that elections in other countries are not better."

The report quotes Matthew Sussex, a Russian foreign and security policy expert, who says: "the Russians have picked up that across the West there is a widespread apathy amongst voters and mistrust of politics and government. Anything you can do to increase that distrust serves Russian interests."

Coverage of events in Ukraine is cited as an example of what it calls Russia's "social media-driven campaign." In a case of the pot calling the kettle black, the report says, "Since 2014, Russia's online information warriors flooded social media with fabricated reports or doctored images of atrocities allegedly committed by the Ukrainian forces [...] Exploiting the fact that information on social media is often conveyed through images, pro-Kremlin [media] widely portrayed Ukraine and Ukrainians in contexts of fascist symbolism and violence." This is tantamount to schoolyard bullying to divert attention from the need to analyze the dangers that the U.S., Canadian and NATO policy of resurrecting neo-Nazis in Ukraine and encircling Russia pose in order to safeguard the cause of world peace. Those who do not accept U.S. imperialist Cold War definitions of peace through strength and the use of force to sort out contradictions internationally and threats and bullying as forms of use of force are not dupes of foreign powers. To establish otherwise by using police powers to criminalize human conscience and speech is a very desperate and pathetic attempt to preserve a rule which does not have the consent of the governed.

NATO's Cyber Activities

The NATO report delineates measures taken by NATO to do "public outreach through social media." The report says NATO has more than 1.2 million followers on Facebook and more than 400,000 on Twitter where it pushes a positive view of NATO that makes it synonymous with defending the Western World.

In the Spring of 2017, NATO launched "We Are NATO," to "explain NATO's core mission of guaranteeing freedom and security," targeting in particular "younger generations in NATO member countries as well as the wider world."

It has also established a website called "NATO-Russia relations: the facts" in Latvia, where a battalion of NATO troops from other countries have been permanently stationed, allegedly to "deter aggression" from neighbouring Russia. This is a country which targets its citizens whose first language is Russian and has passed laws to equate its Soviet liberators from Nazi occupation during World War II with those who joined the Nazi SS.

Anti-Russia disinformation from the Twitter account of Canada's Joint Delegation to NATO in 2014, to justify the NATO military build-up around Russia.

Whereas NATO has always engaged in covert disinformation operations and psyops, such as establishing the organization called the Red brigades, said to be extreme left for purposes of engaging in terrorist acts, it is now doing such things overtly. An example of "overt" information operations through social media incorporated by NATO, during Trident Juncture 2015 exercises, participants trained on "how to quickly produce high volumes of pro-NATO content through official accounts on social media to counter anti-NATO messaging." It claims that as a result of this exercise, "anti-NATO sentiment decreased gradually as the messaging from pro-NATO voices (in local languages) increased."

EU Myth-Busters

The European Union has established two institutions: East Stratcom Task Force and Europol's Internet Referral Unit (IRU) to "counter fake online news and hostile propaganda," news agencies report. IRU is referred to as "EU Myth-Busters" and is comprised of a "team of ten nationally-seconded diplomats, tasked with exposing Russia's online disinformation on a daily basis," disseminating its reports via email and social media. It is said to have a network of "more than 400 experts, journalists, officials, NGOs and think tanks in over 30 countries." In November 2016, the European Parliament adopted a resolution calling for an increase in the Task Force's capabilities.

Germany, France and the Czech Republic reportedly became concerned about "attacks on their political systems" through social media in the run-up to their national elections in 2017 and adopted their own measures.

Eight French news organizations, including Agence France Presse, BFM TV, *L'Expresse* and *Le Monde* teamed up with Facebook and Google to launch new fact-checking tools designed to root out fake news. Any news report deemed to be fake by two of the project's partners is to be tagged.

In the U.S.

2007 press conference held by U.S. Air Force where it announced the establishment of a cyber command to prepare for "victory in cyberspace."

In 2016, the United States' "leading counter-propaganda tool," the State Department's Global Engagement Centre, created in 2011, was "re-branded and strengthened." Meanwhile the Department of Homeland Security has declared the U.S. electoral system "critical infrastructure," facilitating its ability to get involved in "protecting state and local election systems."

In the UK

In the United Kingdom, a dedicated police Counter Terrorism Internet Referral Unit (CTIRU) was formed to deal with content that it assesses as contravening the country's terrorism legislation. Since its inception in 2010, the unit reported getting communication service providers to remove more than 260,000 pieces of what it calls terrorist-related content. In 2015, the British army reportedly created "the 77th Brigade" comprised of experts in the use of social media to conduct "non-lethal information operations" and "counter hostile messaging."

Canada Follows Suit

The Canadian Network for Research on Terrorism was established in 2010 under the auspices of Public Safety Canada to study and "contribute to the global body of knowledge on terrorist use of social media and counter-narrative strategies."

Policing by the Mega-Giants of Social Media

A fundamental feature of the policing apparatus which is being erected is the incorporation of the mega-giants of social media to perform policing services. The NATO report says, "Given the characteristics of the new global information environment, governmental and traditional media actions alone will not suffice. Responsible action by the handful of social media companies that control this medium is critical to the success of the West's efforts."

It goes on to make a number of recommendations: "[C]o-operation with social media industry in order to remove the extremist contents, hate speech and fake news from online platforms should continue, and the most influential information warriors, for instance Russia's chief propagandists, should be subjected to Western sanctions. Since most social media tools are owned by private,

multi-national companies, co-operation with these companies needs to improve. National measures to take down unlawful content are often ineffective because, in most cases, this content is hosted beyond national borders. It is therefore important that the voluntary development and use of anti-trolling and fact-checking software as well as increasing network monitoring by industry be incentivised."

Ironically, having social media corporations "adopt strict internal policies themselves" is viewed as a way "to pre-empt excessive governmental regulations of the cyber domain."

In response, Google has now changed its search algorithms, in effect censoring and/or promoting certain kinds of information. After this change was implemented in April 2017, the World Socialist Website said that its appearance in Google search results significantly dropped, along with those of others, such as Global Research, which NATO's researchers implied is a dupe of the Russians.[1]

NATO's report indicated that in December 2016, Facebook, Microsoft, Twitter and YouTube announced the creation of a shared database of "hashes" -- unique digital "fingerprints" -- for violent terrorist imagery, terrorist recruitment videos and "other images" that will be removed from these platforms. And in June 2017 the same four companies announced the creation of the "Global Internet Forum to Counter Terrorism," said to be an information-sharing platform aimed at making their services "inhospitable to violent extremists."

As of April 2017, in the lead-up to the French presidential election, Facebook had taken action against or removed 30,000 "fake accounts" from its site in France. Twitter claimed to have removed 235,000 accounts for promoting terrorism in the first six months of 2016.

Recently, major social media companies have launched several new initiatives. On December 4, 2017, Google announced it was hiring 10,000 human censors. Human censors have already reviewed over 2 million videos since June, it said. Facebook said it will be hiring 10,000 new staff by the end of 2018 to flag and track fake content. YouTube has removed over 150,000 videos, 50 per cent of which were removed within two hours of upload. The company is working to further accelerate the rate of take-down, YouTube CEO Susan Wojcicki said.[2]

In a discussion of whether the social media mega giants were doing "enough," the NATO report refers to a May 2017 report of the Home Affairs Select Committee of the British Parliament which said social media firms were "shamefully far" from tackling illegal and dangerous content. They are repeatedly "failing to remove illegal content when asked to do so," it said. The Committee urged the British government to consider requiring social media firms to contribute to the cost of the police's Counter-Terrorism Internet referral unit as well as imposing "meaningful fines" for companies which failed to remove illegal content within a strict time frame.

In this regard, German legislators passed the *Network Enforcement Act* (popularly known as the Facebook law) to fine social media and internet technology companies up to 55 million euros if they do not remove malicious content within 24 hours of its being posted. Britain and France are also reportedly working on policies to create a new legal liability for tech companies that fail to take action against unacceptable content.

The NATO report ended with a list of further measures being considered. It included among other things, the study of "best practices" such as the approach used by France's President Emmanuel Macron, "whose skilled technical team thwarted the Kremlin's attempts to harm his [election] campaign" and the creation or designation of specific government units to conduct in co-operation with social media companies round-the-clock monitoring of "detrimental uses of social media, exposing fake news and hostile propaganda, and countering them with facts."

The monopolies who it is claimed will police their own social media networks are the ones who are already known to have assisted the U.S. National Security Agency in violating rights by spying on people, companies and governments around the world through its PRISM espionage program.

Note

1. Sites whose Google search results dropped significantly after Google changed its search algorithms include:

- alternet.org fell by 63 per cent;

- globalresearch.ca fell by 62 per cent;

- consortiumnews.com fell by 47 per cent;

- mediamatters.org fell by 42 per cent;

- commondreams.org fell by 37 per cent;

- internationalviewpoint.org fell by 36 per cent;

- democracynow.org fell by 36 per cent;

- wikileaks.org fell by 30 per cent;

- truthout.org fell by 25 per cent;

- counterpunch.org fell by 21 per cent; and

- theintercept.com fell by 19 per cent.

2. Additional information provided in a December 7, 2017 report on the World Socialist Website:

"YouTube began removing photographic and video documentation of war crimes in Syria in August, terminating some 180 accounts and removing countless videos from other channels, including footage uploaded by Airwars of coalition air raids that have killed civilians, according to Hadi al-Khatib, the founder of Syrian Archive. YouTube later stated that it would work to 'quickly reinstate' any videos and channels that it 'removed mistakenly.'

"In November, YouTube removed over 51,000 videos concerning Anwar al-Awlaki, the Yemeni-American imam who was assassinated via missile raid by the Obama administration on September 30, 2011. Awlaki was never charged with, let alone convicted of any crime. The mass removal was praised by the *New York Times*, one of the largest mouthpieces of the American ruling elite, as a 'watershed moment.'

"YouTube's automated video removal system, implemented in August, places some videos under a 'limited state' which makes it impossible for users to access the videos without already having the URL. Limited videos will not appear in search results, playlists, or viewers' own histories. In addition, the videos can no longer be liked or disliked, commented on (all previous comments are hidden as well), monetized, embedded on other websites, or easily shared on social media through YouTube's share buttons. YouTube has not revealed what criteria it uses to categorize a video as 'extremist' and delist it.

"The company has also begun using automated demonetization to financially censor video producers who upload content it deems 'inappropriate' for monetization, including 'controversial or sensitive subjects, war, political conflicts, natural disasters and tragedies, even if graphic imagery is not shown.' In August, the videos of 'Ron Paul's Liberty Report' were demonetized after a 'manual review' by YouTube found it 'unsuitable for advertisers.' Julian Assange referred to the action as 'economic censorship,' noting that the 'unsuitable' videos featured the former congressman's criticism of president Donald Trump's decision to send more American troops to Afghanistan, as well as criticizing the U.S. Senate Intelligence Committee for branding Wikileaks a hostile foreign intelligence service.

"YouTube has openly admitted on Twitter that it is censoring videos based on content, stating, 'if the video is also not suitable for a wider audience...then it might see poorer performance.

"The system may also pre-emptively flag videos as unsuitable for advertising even before it is uploaded. In the cases where the censorship system cannot evaluate the content of the video -- because it doesn't exist -- it bases its decision on the video's description, tags, and thumbnail.

"The requirements to file an appeal against demonetization are extremely demanding, leaving most small producers with zero recourse. To file an appeal, the channel must either have more than 10,000 subscribers, or the video in question must have at least 1,000 views within the past seven days. Producers are also not informed of when or what in their video the system finds inappropriate. Both small and large producers have complained on Twitter of double-digit percentage drops in new views after their videos have been demonetized, making it even more difficult to meet appeal requirements.

"Google is not alone in its expansion of automated censorship. Last week, Facebook announced its newly implemented system to scan users' posts and contact police and other first-responders, ostensibly to prevent suicide.

"Last month, Google admitted to 'demoting' content from RT (Russia Today) and Sputnik news in its search engine and news service, confirming allegations by the World Socialist Web Site that the company engages in mass political censorship in the name of fighting 'fake news,'" the report's author concludes.

Making Foreign Influence a New Domestic Crime -- The Australian Example

The Australian Liberal-National Coalition government recently introduced a "comprehensive suite of reforms" to counter "the threat of covert foreign interference" in its electoral and political system. The three bills, tabled on December 7, 2017, are currently under committee review where many provisions are being opposed as limitations on freedom of speech, opinion and association.

The *Foreign Influence Transparency Scheme Bill 2017* creates an obligatory registration system for individuals and organizations "undertaking activity on behalf of a foreign principal." The *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* amends the criminal code to include "foreign interference" as a crime against national security. The *Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017* prohibits foreign contributions to political parties and candidates, a common and non-controversial practice in many countries. It goes further, however, extending controls over other associations and organizations, including a new requirement for disclosure of contributors and creating a new registry for "political campaigners."

The legislation was launched at a press conference on December 5, 2017, and tabled in parliament a few days later. At the press conference, Prime Minister Malcolm Turnbull said the legislation tackles a worsening "problem of the highest order," adding that "foreign powers are making unprecedented and increasingly sophisticated attempts to influence the political process both here and abroad." He said the changes to national security laws are required because police agencies "lack the legislative tools they need to act."

In the House of Representatives, Turnbull said that the Director-General of the Australian Security Intelligence organization "is telling us that the threat we face today is greater than when Soviet agents penetrated the federal government during World War II and the early years of the Cold War." He described the three bills as the "interlocking components" comprising "the most comprehensive overhaul of our counterintelligence legislative framework since the 1970s."

In the House of Representatives, Turnbull referred to media reports that "have suggested that the Chinese Communist Party has been working to covertly interfere with our media, our universities and even the decisions of elected representatives right here in this building." "We take these reports very seriously," Turnbull said, going on to identify Russia, Iran and north Korea as other known culprits. "Authoritarian states," he said, "have been literally manufacturing public opinion in order to hijack political discourse and tilt the decision-making landscape to their advantage. And now these methodologies have been turbocharged by cyber."

China's foreign ministry spokesman Geng Shuang expressed shock at Turnbull's remarks at a regular press briefing. "We are astounded by the relevant remarks of the Australian leader," Geng said, according to Associated Press. "Such remarks simply cater to the irresponsible reports by some Australian media that are without principle and full of bias against China. It poisons the

atmosphere of the China-Australia relationship and undermines the foundation of mutual trust and bilateral cooperation. We express strong dissatisfaction with that and have made a serious complaint with the Australian side."

As explained by Prime Minister Malcolm Turnbull, the electoral reforms, the foreign agent registry regime and the creation of "foreign interference" as a crime embody four principles: "sunlight, enforcement, deterrence and capability." The registry will ensure "sunlight" shines on political activities and "allow the public and policymakers to assess any underlying agenda." He said this would give "the Australian public and decision-makers proper visibility when foreign states or individuals may be seeking to influence Australia's political processes and public debates."

Going further, he said that "sunlight" is merely "a disinfectant" and not enough on its own. "We are also introducing, for the first time, offenses for acts of foreign interference. Addressing a clear gap, we will criminalize covert, deceptive and threatening actions by persons acting on behalf of, or in collaboration with, a foreign principle aiming to influence Australia's political processes or prejudice our national security. Acts of foreign interference are often intertwined with espionage. But our espionage laws are so unwieldy they have not supported a single conviction in decades, even as the threat reached unprecedented levels. So we will also introduce a range of carefully structured espionage offences as well as new provisions for secrecy, sabotage and treason."

Referring to the foreign agent registry, Turnbull said, "Being registered, I should say, should not be seen as any kind of taint and certainly not a crime. But if you fail to disclose your ties, then you will be liable for a criminal offence."

Asked by reporters to clarify who would have to register, Turnbull said any organization and/or individual who "thinks they might come within the ambit of the legislation would be wise to register."

Foreign Influence Registry Regime

The *Foreign Influence Transparency Scheme Bill 2017* requires individuals and organizations "undertaking activity on behalf of a foreign principal" to register. Ostensibly, registration would preclude an individual or organization being charged with "foreign influence."

The bill defines a "foreign principal" in detail; summarized as any foreign government, governmental or non-governmental agency, or individual from any foreign country. Critics of the legislation object to this sweeping cover, noting that it captures everyone and everything from a head of state to an unelected political party to the lowliest individual outside of Australia and even non-citizens within the country.

The bill contains an equally sweeping definition of when a person will be deemed to have undertaken an activity on behalf of a foreign principal. "On behalf of" is interpreted as meaning any one of the following: "under an arrangement with," " in the service of," "on the order or at the request of," "under the control or direction of," "with funding or supervision by," or "in collaboration with," a foreign principal. An "arrangement" is defined as "a contract, agreement, understanding or other arrangement of any kind, whether written or unwritten."

What is meant by "foreign interference" in political and electoral affairs is also far-reaching. With some exceptions, it covers anything that aims to "influence, directly or indirectly, any aspect (including the outcome)" of elections, a government decision, proceedings in a House of the Parliament; a process conducted by a registered political party; a process by an independent member of parliament; a candidate, either independent, or of a political party. It also includes

attempting to affect any of these things "by influencing the public, or a section of the public, in relation to the process or proceedings."

The legislation exempts "business and commercial interests" so long as the Australian acting on their behalf acts as an employee or "under the name" of a "foreign business pursuit."

Amendments to the Criminal Code Related to Foreign Interference

The executive summary for *The National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* states that the bill "introduces new offences relating to foreign interference with Australia's political, governmental or democratic processes."

The crime of foreign interference is directly linked with the criminal code's definition of national security, under which there are six criminal activities listed:

> (a) espionage;
> (b) sabotage;
> (c) terrorism;
> (d) political violence;
> (e) activities intended and likely to obstruct, hinder or interfere with the performance by the country's defence force of its functions or with the carrying out of other activities by or for the country for the purposes of its defence or safety;
> (f) foreign interference.

The definition of national security enumerates the broadly accepted concepts of national security, such as defence of the integrity of the country's territory and borders, as well as the territory and integrity of any other country, where Australia has a "responsibility" to do so. The definition also includes Australia's "political, military or economic relations with another country or countries."

There are two categories of foreign interference, one being "intentional" and the other being "reckless," and the proposed legislation distinguishes interference against various targets. "Interference generally" is an offence if:

> (a) the person engages in conduct; and
> (b) any of the following circumstances exists: (i) the conduct is engaged in on behalf of, or in collaboration with, a foreign principal or a person acting on behalf of a foreign principal; (ii) the conduct is directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal; and
> (c) the person is reckless as to whether the conduct will: (i) influence a political or governmental process of the Commonwealth or a State or Territory; or (ii) influence the exercise (whether or not in Australia) of an Australian democratic or political right or duty; or (iii) support intelligence activities of a foreign principal; or (iv) prejudice Australia's national security; and
> (d) any part of the conduct: (i) is covert or deceptive; or (ii) involves the person making a threat to cause serious harm, whether to the person to whom the threat is made or any other person; or (iii) involves the person making a demand with menaces.

Penalty: imprisonment for 15 years.

Electoral Reforms

The *Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017* extends the application of the electoral financing regime to cover a broad range of organizations that the government describes as "political actors that have emerged in the Australian political landscape, who neither endorse candidates nor seek to form government, yet actively seek to influence the outcome of elections through their campaigning activities." While the law already requires organizations and associations spending money during an election to file reports with the Australian electoral commission, the amendments introduce a new category of "political campaigner." It requires any organization that spends $100,000 or more on "political expenditures" in a current year, or any of the previous three years, to register as a "political campaigner" and disclose contributions over $250. "Political expenditure" is broadly defined as "The public expression of any views on an issue that is, or is likely to be, before electors in an election (whether or not a writ has been issued for the election)."

The St Vincent de Paul Society is one of many organizations opposing the legislation. In a brief to the government it stated: "[W]henever a charity comments on issues such as homelessness, low levels of allowances and pensions, low wages, refugees and asylum seekers, electricity costs and a host of other subjects, the costs associated with making these comments would be deemed political expenditure."

Australian Lawyers for Human Rights

The Australian Lawyers for Human Rights (ALHR) is amongst many individuals and organizations opposing the legislation. In a Brief to the Joint Commission on Intelligence and Security, it stated:

"ALHR's primary concern is that [the three bills combined] violate the fundamental universal human rights to freedom of speech and freedom of expression for persons in Australia, and severely restrict the implied Constitutional right to free political communication."

They say the legislation is "neither a proportionate, necessary or reasonable response to the perceived harms of foreign interference in Australia's political and governmental processes and is drafted so broadly that it will have a major impact on ordinary political discourse even where there is only a minimal association between the speaker and a foreign person or entity."

The ALHR states: "While we do not disagree with the aim of requiring recent MPs and recent holders of senior Commonwealth positions to register their activities on behalf of foreign interests, ALHR's view is that the exclusions provided for such persons require clarification, and that the Bill is excessively far reaching in most other respects.

"The Bill provides only a light degree of regulation in relation to business interests but imposes a jungle of regulations and strict liability penalties for non-business interests. The degree of regulation envisaged is completely unnecessary and inappropriate in today's international and inter-connected world.

"Further, the Bill undermines the key role of charities and other non-government organisations in supporting Australia's democracy. The Bill restricts the ability of any speaker with minimal foreign connections to lobby government or even political parties. The very exceptions given to business tacitly recognise the repressive nature of the Bill."

30-Year Career Australian Diplomat Opposes Legislation

Tony Kevin, retired Australian diplomat, has spoken out strongly against the legislation. From 1939 to 1968 he served as a naval officer and wartime intelligence officer. From 1968 to 1998 he was a foreign policy analyst, and also served as Australian Ambassador to Poland and Cambodia. He writes about international affairs.

In his submission on the legislation he opposed the revival of a cold-war atmosphere. He said of himself: "There is large potential for improved relations with Russia, a country which can be admired for its contributions to a rules-based multipolar global order. I want to continue, as a loyal Australian citizen, to work towards the goal of Russia-West detente. I do not regard myself as a foreign agent for Russia and I would resent having to register as such."

His brief states: "As it stands ... this draft legislation is in my view an attack on the freedoms of expression and association that all Australians currently enjoy. I deplore this draft legislation from a civil liberties point of view." He summarized his opposition as follows: "I have no comment to offer on the espionage aspects of this draft legislation. But I do wish to criticize: 1. The draft legislation's philosophical thrust and wording, which ... conflate the traditionally well-defined crime of espionage, with the new presumed crime of 'harmful foreign interference' in Australian government policymaking; 2. The constraints this legislation will put on Australian citizens' present freedoms of expression and free association with foreign persons or organisations; 3.The iniquity of obliging Australian citizens who wish to express views in public on contentious international political issues, and to have contacts with foreign persons or organisations who might share such views, to register as 'foreign agents' as a precaution against their possibly being charged as criminals under this legislation. The arbitrary and open-ended nature of the legislation, which as it stands leaves large discretion to two politicians and Ministers of the Crown -- the Minister for Home Affairs (the new homeland security-style department launched on December 20, 2017) and the Attorney-General -- in deciding which Australian persons and/or actions should be prosecuted as criminal offenders and/or offences under this draft legislation if it becomes law."

"Overall, I find this legislation offensive and dangerous. It threatens my freedom to form and express political views on world affairs, and to visit or associate with individuals or public organisations from particular countries with which Australia has normal diplomatic relations. I hold no official secrets, having been retired from the Australian public service for 20 years. All my information and policy insights come from information freely available to any Australians in the public arena. Why should I not accept invitations to prestigious international non-governmental lecture tours or conferences in Russia or China -- even expenses-paid invitations; speak at them; and write about them afterwards? Why should I not write books or articles on Australia's relations with Russia or China? Why should I not accept royalties from commercial or public organisations in those countries?"