

U.N. Security Council 2030

UC Davis Collegiate Conference

Model United Nations

November 10th-11th, 2012

INTRODUCTION: A letter from the USG of Committees

Greetings, delegates, and welcome to the United Nations Security Council 2030!

Like in any committee, you will be debating, compromising and proposing solutions to crises gripping the world and hopefully preserving a state of peace and security. Unlike most committees, however, this one takes place eighteen years removed from our own time. Since none of us have psychic powers, least of all yours truly, conducting research outside this topic guide is going to be difficult if not impossible. I will do my best to be as comprehensive as possible in the following pages, but if there’s anything you want to know about your country’s policy or the situation in general, you can email me at brendan.obrien@davismun.org with any questions. Please put “UNSC 2030” in the subject line; I’m not going to be touchy about that, but it will make my life a whole lot easier as I sort through things. I will check my email more frequently as the conference gets closer, but I will make sure all your questions get answered in a reasonable time frame. If the question is particularly relevant to everyone, I can send it out to the other delegates so everyone can benefit.

The situation presented here is something I’ve developed on my own. Some of the inspiration comes from a few other sources, most notably George Friedman’s The Next 100 Years (which uses geopolitics to make a lot of very interesting, if unusual, predictions about the state of world affairs in years to come.) Nothing comes directly from the book, but I used some of his methods to set up the situation. I can’t say I recommend reading it as research, but if you wish to take a look at it, either to learn something about geopolitics or just to try to get inside my head, you’re more than welcome to do so. Again, most of your research is going to consist of the topic guide and whatever you email me about.

The committee itself will run like a regular Security Council committee. For those of you unfamiliar with what this means, that means that it’s going to be very fast paced and crisis-oriented. Due to the nature of the beast, as it were, we won’t diverge too widely from the topics at hand since there’s no outside information to draw from, but do keep in mind that the unexpected can and will happen. Other than that, the one form of outside research I do recommend is reading up on the structure of the Security Council and where its powers lie if you aren’t already familiar with those things. The basic charter and goals of the Council have not changed.

Finally, when formulating your policies, other than what’s described within, assume that not too much has changed. I’ll try to discuss anything that would cause a large re-evaluation of your nation’s defensive priorities in here, so you can assume that you generally have the same national interest as now other than what’s described. Since each country will have information about how it fits into the world at large, it’s otherwise fairly safe to assume status quo. If you’re not sure, feel free to email me and ask.

Now that that’s out of the way, let’s visit the world of tomorrow. Best of luck, delegates!

Sincerely,

Brendan O’Brien

Undersecretary-General of Committees, DMUNC 2013

**TABLE OF CONTENTS**

1. THE WORLD IN 2030

Topic One: North Korean Crisis

Topic Two: Australian Cyberterrorism

Background Information: Cyberwarfare and the White Hand

Background Information: Nuclear Proliferation

Background Information: The Arab Spring, Nineteen Years Later

1. MEMBER STATES

United States\*

Russian Federation\*

United Kingdom\*

France\*

China\*

India

Brazil

Japan

Germany

Egypt

Republic of Korea

Morocco

Australia

Iran

Mexico

\*An asterisk indicates a permanent member.

NOTE: HOW DO I RESEARCH?

It may be helpful to read up on countries you expect to work with or against, but above all else be familiar with your own policy. If you have a question about whether something is on- or off-policy, feel free to email me, but if you’re stumped, assuming status quo is a good option. A sensible way to go about this would be to research your country’s response to similar situations in the past and try to intuit how it might react to the crises at hand. For this reason, on- and off-policy decisions aren’t as clear-cut as in a regular committee. Do your best given what’s in here, and email me if you need to fill in any other gaps. Please feel free to email me about anything I may have omitted or specific questions about your policy. This committee is definitely an experiment, so help from all of you will only make it better.

TOPIC ONE: NORTH KOREAN CRISIS

When Kim Jong-un ascended to power in late 2011, most of the world had little idea of what to expect. As the world’s youngest head of state, the new leader earned a great deal of international scrutiny after his botched handling of a missile test that resulted in little but withdrawal of badly-needed food aid (1) offered by the United States (2). In response to increasingly rampant floods (3) and this absence of food aid, Kim’s policies in the following years were designed to accept increasing diplomatic isolation while simultaneously trying to implement economic reforms. The most notable of these was the partial repeal of Kim Jong-il’s disastrous “military first” policy, under which a great majority of the country’s resources were given to its massive standing army, leaving its people to starve. Kim attempted to model his new policies after the “Juche idea” espoused by the country’s revered founder, Kim Il-sung; indeed, state media constantly referred to them as the “New Juche Idea” after one of Kim’s addresses to the Korean People’s Army in 2014 (4).

As he seemingly brought in increasing amounts of foreign culture and ideas, most notably shown by his apparent love of Mickey Mouse (5) and a much-discussed concert in Pyongyang by South Korean girl group Girls’ Generation (6), he doubled down on increasing food production to help feed the citizenry. While he did indeed increase his country’s domestic food production by just over ten percent in only seven years, these gains were offset almost entirely by losses in foreign aid as his several provocations of South Korea via missile and ballistics tests left his regime diplomatically isolated. (7) His seemingly contradictory policies of trying to present a more “respectable” and economically liberal North Korea to the outside world while brazenly pursuing his nuclear weapons program and missile tests alienated not just the international community but many of his officials in the army and Korean Worker’s Party. Kim Jong-un went on at length about the impending Chinese-style economic reforms he supposedly longed to implement, but never took any other visible steps to do so..

The first visible crack in the regime showed on January 21st, 2020, when an anonymous interview with the Associated Press from an official who detected to Seoul was published. In addition to publicly leaking information such as location and operational details of prison and labor camps and the true scope of the nation’s food shortages, he gave an impassioned appeal for foreigners to stand up to what he called “the devils that run my country.” An excerpt is reproduced below:

“Do not be fooled by the charade of opening to and acceptance of the outside. The country is run by the same devils that have ruled it for years and years. The tyranny always remains, only its face changes…Even if my name was revealed, I no longer care. Let the devils come. They have no power over me anymore.”

 -Anonymous

 Three days after the interview was published, the Korean Central News Agency announced that Vice Marshal Choe Ryong-hae had “fallen seriously ill” and was to be removed from his position in the Politburo immediately. He was never seen in public again; to this day, what exactly happened to him is unknown, though he is presumed dead. Though suspicions ran rampant that Choe was the mysterious defector in the interviews, given the timing of his disappearance, a nationwide ratcheting up of already strict government suppression prevented any investigation outsiders may have wanted to conduct. At least two hundred journalists disappeared in the ensuing weeks, though the real count may have been as high as 1,500. A massive purge of high-ranked party officials followed for nearly a year, leaving the elite of the Worker’s Party of Korea and the officials in the Korean People’s Army largely replaced. The purged officials were supposedly shipped off to the “kwan-li-so,” or political prison camps (8).

 In the aftermath of this incident, fueled by additional braggadocio in July claiming that the state “would continue plutonium enrichment whether the imperialists wish it or not,” international aid dwindled to near zero. A comprehensive round of sanctions was passed by the Security Council in September; even the People’s Republic of China abstained on the grounds that Jong-un “seem[ed] more concerned with anatagonizing others than his nation’s own self-preservation…This instability is a threat to both China and the world,” in the words of President Li Keqiang. Kim Jong-un seemed shocked at one of his closest allies, or at least a nation high on the list of those willing to even engage with him, would act in such a way. Several nations’ intelligence recorded him as privately ranting and raving at accusations of Chinese “betrayal,” though no such accusation was ever delivered through state media (9). In response to the sanctions, he doubled down on his self-sufficiency policies. Calling for “a revolution eternally grounded in the traditions of our forefathers,” he began reversing his economic reforms and declared that the economy should focus ninety percent of its production capabilities on food and weapons, “cutting out decadent luxuries and producing only what is required for the nation’s continued prosperity.” Other kinds of factories were shuttered en masse as workers from the cities were moved out to collectivized farms and rural inhabitants were moved to the remaining arms factories in the cities. The armed forces, of course, stepped in to “correct” the choices of those who would have created an imbalance in the labor force. The “military first” policy, supposedly abolished only seven years earlier, came back in full force. Falls in food production amounted to less than half of one percent, but the actual living standards of North Koreans fell precipitously. Riots on the streets of Wonsan and Kaesong in January 2025 could not even be suppressed by state media, painting an increasingly bleak picture of a regime that was rapidly unraveling at the seams. Officials were installed and expunged as if the whole of the Worker’s Party of Korea was a giant revolving door. Generals and other elite officials in the Politburo spoke out less and less out of fear of saying the wrong thing and getting sacked, which occurred on a frequent basis. Rumors circulated that some of these generals were beginning to doubt in Kim’s leadership, but considering the domestic turmoil, little was to come of them for the time being.

 In the aftermath of the riots, much of the international community was left perplexed as to what course to take. Chinese politicians called for “stability above all else” and Li Keqiang repeatedly called on Kim Jong-un to take steps to ensure that he could prevent his country from slipping into anarchy, warning that “turmoil enables our enemies” in what many interpreted as a fear of losing an important buffer against American troops in South Korea. The response from Seoul was varied; the ruling liberal Democratic United Party saw the turmoil as an opportunity to provide assistance and increase influence in a revival of its old “Sunshine Policy,” but the conservative Saenuri Party claimed that its opponents were delusional and negotiation was useless. When an aid package advocated by South Korea through the United Nations World Food Program and an economic agreement in concert with the United States and European Union were rebuffed, the Saenuri Party’s line of thinking proved popular with the voters, and the party swept into power in 2027 and governs to this day. U.S. President Julian Castro expressed sympathy for the rioters in a speech that is partially reproduced below:

The United States and the world hear the anguished cries of the North Korean people, even when their own government does not. Kim Jong-un would be wise to not turn a deaf ear and put his own pride above the welfare of his People, for so-called “leaders” who took that path have never prospered.”

 -Julian Castro, Feburary 3rd, 2025

For four more years, the regime struggled on. The government was purged nearly continuously as Kim Jong-un struggled to maintain control over a country that began to openly despise him and an army that increasingly refused to trust him. A band of mid-level army officers, calling themselves “Comrades of Choe Ryong-hae,” openly refused to participate in riot suppression operations in Pyongyang in June 2028. They were, of course, swiftly executed, but their defiance became symbolic to both disgruntled party officials and the common folk. Small bands of defectors traveled the land, telling the common folk the truth about the atrocities and incompetence perpetuated by the regime, hoping to radicalize them into open revolt. They mostly failed and were shot on sight, but the seeds had been planted and would soon germinate and bloom.

 Three weeks ago, on September 22nd, 2030, the prisoners at Kwan-li-so Number 15 near the city of Yodok assaulted the guards and stole their weapons, breaking free from the camp and fleeing southwest in the apparent direction of Kwan-li-so Number 18. Military commanders stationed in Yodok refused to pursue them. Four days later, an attempt on Kim Jong-un’s life at a Worker’s Party of Korea assembly in Pyongyang nearly succeeded, causing the leader to flee with two of his most trusted generals. Hours afterwards, KCNA reported that the Respected Leader “had been threatened and was being moved to a secure location.” In the middle of the broadcast, however, the transmission was cut short and a transmission from Admiral Pak Jung-sun of the Korean People’s Navy proclaimed that Kim Jong-un had abdicated and that the admiral had been appointed the new chairman of the Korean Worker’s Party. He declared that the government would immedately accept any and all food aid and security assistance and would, in exchange, hand over all of its enriched plutonium, rewrite the country’s constitution, institute economic reform and never perform another missile test in violation of international law. The authenticity of his claim was dubious, but many in the army rallied to him, seeing him as the best chance to save their nation. Li Keqiang endorsed him almost immediately and the People’s Republic of China has submitted a request to the Security Council to his effect. South Korean and later international media labeled Pak and his supporters the “Sunshine Faction (Korean: 햇볕정책자,)” for their seemingly engaged policy to the outside rather than Kim Jong-un’s radical isolationism.

 The escaped prisoners from the labor camp, with assistance from several defecting army colonels, have liberated two other camps in the previous weeks, and many from the cities and beyond have rallied to their cause. Calling themselves the “Unionist Movement (Korean: 통합론주의자,)” these rebels call for reunification with South Korea immediately. Carried forward by a great deal of popular goodwill and effective use of mobile communication and guerrilla tactics, they vow to bring down the oppressive state in any form, whether it be the remaining followers of Kim Jong-un or Admiral Pak and his conciliatory attempts to keep the country together. The political opposition, especially the minority Korean Social Democratic Party that operated openly but with no power under the old regime, embraced the movement, claiming while unification may not “give everyone everything they might want,” it was the only way forward and to allow some form of freedom in the land. Leaders including British Prime Minister Edward Miliband, French President Jean-Francois Cope, and U.S. President Juilan Castro have expressed sympathy with their goals, though no leader has yet officially declared support for them. South Korean President Lee Soo-yeon has praised the Unionists’ efforts since the government learned of them and is expected to release a statement officially backing them within the week.

Kim Jong-un, lost in the chaos for approximately a week, reappeared in Hwasong on October 7th, 2030 with several of his generals. He broadcast that he was still the sole leader of the country, though the dual insurrections under the Unionists and the Sunshine Faction made that claim laughable. Even so, he still commands a portion of the army roughly equal to the one loyal to Admiral Pak and significantly larger than that of the Unionists. His goals seem to be to ensure that neither other faction gains control of the nation, though beyond this they remain unclear; after *Pravda* reported that an appeal to Russian Federation President Dimiti Medvedev and Prime Minister Vladimir Putin received an inconclusive answer, he has not communicated with the outside as of yet, at least in any way known to the international community. As he already has access to a great deal of the army’s resources, he currently seems to have the best position on the ground, though information is still fragmented and unreliable at this time.

Several unsubstantiated reports call into question how well Kim Jong-un and his supporters control his stockpile of plutonium and other elements of his nuclear program and what exactly he might do with them, but no credible intelligence known to the international community has emerged at this time. The best current estimations place the amount of usable fissile material the regime possesses at around 140 kilograms (10). North Korea still has no known silo-based launching systems, so the material could be anywhere. That said, no representative of the Unionists or the Sunshine Faction has announced control of any of this material, so it likely remains in regime hands, though exactly where it is stored is unknown. The nation’s maximum tested missile range is approximately 5,600 kilometers from the three-stage Tape’o Dong-1, which would be enough to strike at the Alaskan coast (11). While it seems unlikely that Kim Jong-un would use nuclear weapons on his own lands, it would nevertheless be prudent to keep the state of this weapons-grade material in mind, as in the wrong hands it could pose a grave threat to international security.

The Security Council is called to order at this time of great crisis to formulate a coherent international response to this disorder. As chaos rages on the ground, many people are likely to die and turmoil has the possibility of spreading. The world watches as one of the world’s cruelest dictatorships crumbles and turns to the Security Council to ensure that strife and bloodshed are cut short, one way or another. Delegates, you must not fail.

Footnotes:

(1) <http://en.rian.ru/world/20120413/172792442.html>

(2) <http://www.economist.com/blogs/banyan/2012/03/north-korean-nuclear-progress>

(3) <http://www.economist.com/node/21560305>

(4) “Juche” translates roughly as “self-reliance.” I have tried my best to have accurate translations throughout, but I sadly do not speak Korean; thus, they may not be one hundred percent correct. My apologies.

(5) <http://drezner.foreignpolicy.com/posts/2012/07/10/kim_jong_uns_kryptonite>

(6) <http://www.youtube.com/watch?v=L05wn7w0Rz8>

(7) Among other things, pressure from the South Korean government in the aftermath of a 2016 test of a two-stage Tape’o Dong-1 missile resulted in SM Entertainment cancelling the remainder of the tour following the Pyongyang concert.

(8) <http://freekorea.us/camps/>

(9) For an explanation on the change in Chinese strategy that led to this change in policy, see the following: <http://nautilus.org/publications/books/dprkbb/china/dprk-briefing-book-china-and-the-korean-peninsula-beijings-pyongyang-problem-and-seoul-hope/>

(10) Projected forward from <http://nautilus.wpengine.netdna-cdn.com/wpcontent/uploads/2011/12/CIAEnrichmentNov-02.pdf>

(11) [http://en.wikipedia.org/wiki/File:DPRK\_missile\_ranges.jpg](http://en.wikipedia.org/wiki/File%3ADPRK_missile_ranges.jpg)

TOPIC TWO: AUSTRALIAN CYBERTERRORISM

As governments and economies have become increasingly integrated with virtual systems, attempts to subvert these systems for political and personal ends have also increased. The first major attack in recent memory that entered popular consciousness was the use of a worm called Stuxnet (1) to overload some of Iran’s nuclear facilities (2). Since then, the code for Stuxnet and similar worms has proliferated like wildfire (3). Despite the potential demonstrated by this attack, states were slower at adapting countermeasures than cybercriminals and state-employed hackers were at developing them. Untold amounts of crucial information is stolen daily, whether for profit or to punish enemies. While information theft is a vital problem to member states, the international community as a whole and the Security Council in particular is greatly concerned with the physical damage sophisticated cyber attacks can cause. By shutting down or interfering with computer systems that oversee the operations of banks, farms or power plants, great economic and physical damage can result. As the world becomes ever more computerized, from labor mechanization to transport automation, cyber attacks grow in potential danger by the year. One of the important developments of the generally failed United Nations Convention on the Laws of Cyberwarfare of 2020 was the incorporation of the United Nations Special Envoy on Cyberwarfare into a permanent subcommittee of the Security Council. Thus, taking action against acts of cyberwarfare and cyberterrorism to ensure keeping international peace falls within the council’s intended purpose and will be necessary to ensuring a secure future.

It is generally very difficult to pinpoint the exact cyber-capabilities of a nation. A well-executed cyber attack is virtually impossible to trace and the nations involved obviously keep these capabilities classified, lest their effectiveness be countered by patching security holes in systems. Nonetheless, the People’s Republic of China (4) and the United States (5) are regarded as having the greatest capabilities for both cyber attacks and countermeasures, likely in that order. While most developed nations and emerging economic nations have some form of cyber capability, none have the manpower devoted solely to cyber activities to match either of these two. By many estimations, Iran and the Russian Federation are the next closest with regards to estimated capabilities.

As with the rise of terrorism as a major global force in the early twenty-first century, non-state actors rapidly developed new and deadly capabilities to sabotage networks that have generally outpaced state efforts. One of the first examples that gained worldwide prominence was the group Anonymous, a loosely organized group of hackers that repeatedly infiltrated secure networks of corporations and other organizations (6) and posted classified information (7). While the group still exists today, its methods are “behind the times” in both complexity and severity. Anonymous caused many organizations and states grief by posting classified information and launching attacks on their websites, but never posed a serious threat to international security. Modern groups, such as the Australian ultranationalist terrorist organization known only as the “White Hand,” are much less principled and more lethal in their methods.

 Modern cyberterrorism techniques can be traced to the birth of the White Hand in Darwin, Australia. Fifteen years ago, a local gang with white supremacist views known as the “Slitherheads” that mainly engaged in drug manufacture found its market drying up in the face of increasing government crackdowns on illegal substances. Looking to keep a steady source of income, the group turned to cybercrime, notably stealing the email account passwords of several hundred local government employees and selling access to the accounts at a premium. The gang used the profits of each raid to pay for increasingly skilled hackers and better code until, within a few years, they had the cyber attack capability roughly a match for the entire defense capability of an average security firm. The group’s egotistical leader, a man known only as Seth, looked at the increased income and decided to “go global,” as he put it in a Youtube video directed at like-minded individuals. Rebranded as the White Hand, the organization would become a group of “hacktivists” dedicated to attacking individuals, corporations and nations they saw advancing the cause of racial harmony.

Three months after the video was posted, on January 1st, 2019, the organization launched a massive distributed denial of service (DDoS) against the websites of the Royal Australian Air Force and Royal Australian Navy, the Department of Foreign Affairs and Trade, and the Australian Labor and Liberal National Parties that left all affected sites down for nearly four days. They immediately claimed credit and warned that further and more devastating attacks were to follow. The Australian government immediately launched an investigation, capturing several members but neither Seth nor any of his direct underlings. Despite its losses, the White Hand regrouped with its first deadly attack two years later on the nation’s first and only nuclear power plant near Perth two years later, built under the pro-nuclear Liberal National government in 2015. The worm it used, L-1, apparently used a security key stolen by an advanced version of the Duqu worm developed by the group that created Stuxnet (8). Once introduced, L-1 caused the plant’s cooling systems to shut down, eventually causing a meltdown. While cleanup efforts were fast and relatively effective, hundreds died and thousands more were exposed to dangerous radiation levels. The manhunt for the members continued, but proved frustratingly inconclusive. For each member that the government captured, there seemed to be two more to take his place. After this incident, Australia, the United States, the United Kingdom and the People’s Republic of China branded the White Hand a terrorist organization. A majority of UN member states followed suit.

While the White Hand was a white supremacist organization devoted to destabilizing the Australian government for supposedly being “soft on immigrants, refugees and minorities,” after the Perth nuclear disaster the organization quickly fell under the dominance of radical members of the Japanese Aum Shinrikyo cult, currently known as Aleph (9). Apparently, the two groups had an interest in common: inflicting a devastating attack on the United States. According to Aum Shinrikyo’s original mythology, the U.S. is the incarnation of Satan and will begin an apocalyptic nuclear war that the cult’s members will survive. (10) The White Hand loathes the United States for its widescale application of the virtues its members hate the most: multiculturalism and integration. A bargain was struck: Aleph would provide all the funding the White Hand’s skilled hackers needed to bring the United States to its knees, the methods of which each group could then use on their home nations. (11)

 The precise timing of these events is unknown, but the best intelligence available indicates that the groups had contact in early 2022 and spent the next three years preparing for an attack. On March 1st, 2025, the White Hand released a video promising that March 20th would “be known to all people as the Day of Terror. We shall watch the world burn and spit on your pleas for mercy (12).” Seth degenerated into a largely incoherent rant for the remainder of the video, but his initial message remained clear. Governments all over the world took precautionary measures, and the U.S. Secretary of Defense offered the full assistance of the United States Cyber Command to Australia in stopping any potential attacks.

 The security experts had bargained that, given the success of their attack using the L-1 worm and Seth’s supreme egotism, whatever the White Hand was going to unleash would be a derivative of this worm rather than an entirely new creation. Thus, resources were disproportionately devoted to looking into L-1’s design and developing countermeasures. A joint commission by American and Australian cyber operatives managed to develop a patch that rendered the method that L-1 used to obtain security keys useless on March 14th. It could not be adapted to all likely targets quickly enough to eliminate the threat, but it is generally agreed that it prevented a great deal of damage. The “Day of Terror” mostly consisted of a rash of attacks on American power plants. They were successful enough to leave a good deal of the American eastern seaboard completely without power for a good five hours, but thanks to the concentrated Australian-American effort it was far from the dramatic show of force that the White Hand had in mind. Indeed, analysis of the events found that code for the worm the White Hand used, unimaginatively dubbed “L-2,” had inserted itself into computers that dealt with low-security information at NORAD’s Cheyenne Mountain installation. While these attacks were thwarted, they put the White Hand in the position of being the most dangerous group of cyberterrorists in history, representing a grave national and international security threat.

 The White Hand remained relatively quiet for the next three years, a development presumably aided by drying-up Aleph funding in the wake of a comprehensive Interpol investigation of Aleph members working with the White Hand. Nevertheless, on Christmas Eve, 2028, Seth posted yet another video from an unknown location. This time, he promised that he had “declare[d] war on the bloated corpse known as the Australian government.” He called on his followers to unleash every form of attack they could muster. The video even ended with an ominous call for an armed uprising. Given the seemingly supernatural capability of the organization to infiltrate systems, especially its frightening intrusion in Cheyenne Mountain, the Australian Parliament passed a series of laws that made internet monitoring significantly easier and significantly easier to obtain a warrant for. Internet activists called it a massive infringement of civil rights, but Prime Minister Bruce Jones of the Liberal National Party promised that the law would be allowed to expire in two years’ time and that much of the population was legitimately scared of what might happen, given the strong memory of the Perth incident.

 Unfortunately for all, the White Hand made good on its word. Much of the Northern Territory and parts of other Australian states have been plagued with rolling blackouts for nearly a year; only several months ago were they brought under control. So many emergency generators were sold over this period that their electricity production, for a brief period in September last year, actually outstripped the Northern Territory’s crippled electric capacity. Compromised internet and other government communication services have periodically disrupted Australian naval exercises in the area as commanders find themselves unable to direct their troops. A new, entirely automated maglev line between Darwin and Alice Springs had to be shut down due to the fact that constant attacks on its control systems have rendered it basically inoperable. Most frighteningly, gangs armed with assault weapons claiming to be White Hand affiliates have staged shooting rampages in areas around Darwin inhabited primarily by non-white Australians. The death toll in these shootings amounted to nearly 1,800 as of October 1st of this year; while they have mostly ceased, there are still many victims unaccounted for. The government has declared a state of emergency that was only lifted on August 15th of this year due to the brutality and omnipresence of these attacks. As the violence and other operations begin to die down, Australia has emerged as a scarred and shaken nation. Popular opinion is overwhelmingly against the White Hand, meaning that their racism fortunately find less of a voice than ever in Australian politics. Feeling that its sovereignty and security are threatened, Australia calls upon the Security Council to take action against the White Hand and the legions of cyberterrorists like them.

Perhaps the most terrifying idea of all, and the one delegates would be the wisest to consider, is that this may only be the beginning. As horrid as these attacks were, they were still ultimately conducted by one isolated group. A state engaged in a full cyberwarfare effort would be capable of even more frightening attacks. In addition to taking steps to ensure that Australia will be safe from future attacks from the White Hand, whatever those steps might entail, many member states advocate establishing protocols to deal with future acts of cyberwarfare and cyberterrorism. Decisive action would put the United Nations in a unique position to stop and mitigate these acts so what is coming to be called the “Australian Terror” will not be repeated elsewhere. The future of cyberspace may very well be in your hands, delegates. Good luck.

Footnotes:

1. <http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html?pagewanted=all>
2. <http://www.youtube.com/watch?v=scNkLWV7jSw>
3. <http://www.nytimes.com/2011/10/19/technology/stuxnet-computer-worms-creators-may-be-active-again.html>
4. <http://en.wikipedia.org/wiki/Cyberwarfare_in_the_People%27s_Republic_of_China>
5. <http://www.defense.gov/news/newsarticle.aspx?id=60869>
6. <http://en.wikipedia.org/wiki/Timeline_of_events_involving_Anonymous>
7. <http://www.aljazeera.com/indepth/opinion/2011/03/20113981026464808.html>
8. <http://www.japantimes.co.jp/text/ff20020327a1.html>
9. <http://www.nytimes.com/2011/10/19/technology/stuxnet-computer-worms-creators-may-be-active-again.html>
10. http://en.wikipedia.org/wiki/Aleph\_(religion)
11. For more on the White Hand, see “Background Resource: Cyberwarfare and the White Hand.”
12. March 20th, 1995 was the date of Aum Shinrikyo’s deadly sarin gas attack on the Tokyo subway system. This is likely why the White Hand chose this date and has been pointed to by investigators as proof that the groups’ association should have been deduced sooner.

BACKGROUND INFORMATION: CYBERWARFARE AND THE WHITE HAND

Cyber attacks have become an integral part of the offensive and defensive capabilities of modern nations and non-state actors. Here are basic definitions of important cyberwarfare terms. It would also be prudent to research more into your particular nation’s cyber capabilities.

* Denial of service (DoS) and distributed denial of service (DDoS) attacks: This form of cyber attack seeks to shut down a certain computer or server by bombarding it with more traffic than it can handle. A system with an overload of traffic requests will be unable to function, thus denying others the ability to access the site or network. Distributed denial-of-service attacks differ from regular denial-of-service attacks in that they use multiple systems working at once to accomplish these tasks.
* Firewall: A barrier designed to regulate incoming traffic to a network based on its perceived safety. These form a key component of cyber defense.
* Virus: Malicious code that is inserted into a given computer that is designed to impair its functionality or corrupt files.
* Worm: Malicious code that is inserted into a given computer that is designed to copy itself and insert itself into the host computer’s own code, whereupon it may perform or override various functions. They differ from viruses in that their primary purpose is to change code rather than delete or simply damage it.
* Zero-day vulnerability: A hole in security that a system’s manufacturers are unaware of and thus do not have security measures in place against. Due to their obvious utility in circumventing a system’s defenses, knowledge of zero-day vulnerabilities can fetch obscene prices on the black market in the range of hundreds of thousands to millions of dollars.
* Zombie: A zombie computer is one that has had control compromised by an outside source (likely via a worm) and is used to launch cyberattacks without knowledge of its owner. Computers in this state can be issued commands remotely to flood sites with traffic or perform other tasks.

The following is taken from a declassified report from the Australian-American commission created to prepare defenses for the “Day of Terror.”

“The White Hand is an internationally recognized terrorist organization apparently based in Australia’s Northern Territory, though its influence extends throughout the nation and has some amount of strength in the United States, New Zealand, and Japan.

The group’s exact membership and structure are unknown, but the man known as ‘Seth’ does appear to have some degree of authority within the group. Whether is a figurehead or the actual leader is unknown, though a central leader would be consistent with the Slitherhead gang that the White Hand emerged from. Judging by the fact that each of Seth’s videos and transmissions appear to be of the same person with the same voice, it appears that he is one person and not a mascot. As virtually all captured White Hand operatives have some knowledge of him, it would appear he does issue a significant portion of orders. Below him, there are three individuals known as the ‘Troika’ that seem to be tasked with conceptualizing and designing the operations. Australian police managed to capture one of these men in 2024 with Interpol assistance, a man known as ‘Jaeger.’ He was identified as [CENSORED], a native of Brisbane, Australia who supposedly ran a carpentry business. ‘Jaeger’ revealed the existence of the Troika and the codenames of the others, ‘Berthold’ and ‘Selvaria,’ though he did not seem to know their actual identities. This suggests that Seth gives orders to each of the Troika separately and that the cells operate separately. This again points to Seth having central command of the organization. The remainder of the organization appears to be organized into cells, which the Troika seem to have some amount of (but apparently not total) influence over. He claimed that as many as 10,000 members serve his cause between the three cells, though this number seems extraordinarily high. Perhaps he was referring to people whose computers the organization had compromised. This body estimates membership at close to 2,000, with about half of those members representing some sort of cyber threat. ‘Jaeger’ provided this information in exchange for limited charges; he is currently serving 15 years in prison.

Though we cannot confirm it at this time, we have suspicions that the organization’s seemingly disproportionate capabilities relative to its size can explained via covert funding from a number of wealthy citizens. Most are Japanese, with a few nontrivial contributions coming from locations in Russia. We have roughly pinpointed their countries of origin but not all of their identities. The two members currently apprehended, [CENSORED] and [CENSORED,] were connected to the Aum Shinrikyo cult that launched a sarin gas attack in 1995. We do not as yet have enough evidence to pinpoint all of that organization’s involvement, nor can we ascertain their exact motive for funding such a group. We recommend an investigation into the matter.”

-Australia-New Zealand-United States Emergency Cyberdefense Commission [ANZUS-ECC], March 2025 Report

BACKGROUND INFORMATION: NUCLEAR PROLIFERATION

The number of nuclear weapon states allowed under international law has not changed in the past twenty years. France, the Russian Federation, the People’s Republic of China, the United Kingdom and the United States remain the only states officially allowed to have nuclear capabilities under the Nuclear Non-Proliferation Treaty.

In practice, however, this enforcement has not prevented other states from acquiring atomic weaponry. The following states are widely believed to also have capable nuclear launch capacity in some form.

* India
* Iran (1)
* Israel (2)
* North Korea (3)
* Pakistan

Footnotes:

1. Despite widespread speculation on an Israeli attack on Iranian nuclear facilities if it got close to developing a nuclear bomb, no such attack occurred. Neither Israel nor the United States issued a statement on the subject. Despite the international community’s best diplomatic efforts, Iran completed a nuclear test in 2015 but to this day has neither confirmed nor denied having an actual nuclear weapon. Government ministers claimed that the test was for “peaceful nuclear purposes.”
2. Israel is widely believed to have these weapons, though it has neither confirmed nor denied this.
3. North Korea’s current nuclear capability is described in more detail in Topic One.

BACKGROUND INFORMATION: THE ARAB SPRING, NINETEEN YEARS LATER

The following is taken from the week of September 24, 2030 issue of *The Economist.*

“So what, exactly, have those brave revolutionaries accomplished in twenty years? In some ways, a great deal. Libya, in particular, quickly established order and strengthened its economy with its new democratic institutions. The Muslim Brotherhood did not seize power as many feared, and while it has dominated Libyan politics in recent years, the liberal parties have been heard. They even won their first presidential election this year, which seemed unthinkable a very short time ago. Certainly, oil revenue has played a role in this prosperity, but a legitimate democracy backed by oil is still a legitimate democracy. The nation celebrates its fourth round of internationally declared free and fair parliamentary elections later this year…Egypt, too, has made the transition to democracy quite well, despite often persuasive calls from Salafists for the imposition of Sharia-based laws. The Muslim Brotherhood has remained in government from the first elections until now, yes, but they have had to share power and establish strong democratic institutions and the rule of law. When Egypt was elected to the Security Council this past year, the nation that took on that responsibility was ready to take on the task of defending peace and freedom…

In other ways, though, not so much has changed. In Yemen, barely a day goes by without a new warlord rising to challenge the central government – and they often would have a fighting chance of winning if not for the United Nations and Arab League providing massive assistance to the rapidly degenerating state. Syria emerged from its revolution in a “lake of blood,” as we put it years ago, and has had a fractured government that is paralyzed along sectarian lines. Bashar al-Assad was defeated, but at a titanic cost in both blood and treasure. Syria is better off than it was under its old regime, certainly, but it still has a long way go before it can join the rising Arab community of prosperous and peaceful democracies…

In summary: Did the Arab Spring bring real change? Certainly it has, and perhaps irrevocably so. On a grand scale, it could also be said that this change has certainly been for the better. But for some countries, change has meant more than it has for others.”