THE INTERNATIONAL CRIMINAL POLICE ORGANIZATION:

Policing Online Spaces

INTERPOL

COLLEGE OF THE CANYONS

MODEL UNITED NATIONS CONFERENCE

2022

General Assembly Background Guide

Table of Contents

Letter from the Secretary-General

Welcome, Esteemed Delegates!

My name is Samantha Dalton and it is my absolute honor and privilege to serve as your Secretary-General for COCMUN 2022, and furthermore to present you with this fantasmic conference!

A little about me, I am a sophomore in my last semester at College of the Canyons dual-majoring in Political Science and Legal Studies. Additionally, I am the Head Delegate of COC's very own Model United Nations Team as well as a member of a number of clubs and organizations on campus such as the Associated Student Government and Political Science Club. Outside of academia and its relatives, I enjoy traveling, reading, and spending time with those that mean the most to me. Amongst these things, I can say that it has truly been a wonderfully crazy experience working with such a talented and ideologically diverse group of individuals in order to ensure that not only we would host this conference but host it in an in-person medium after many long months of Zoom fatigue.

I am truly excited to see the creative solutions delegates will develop and debate over the course of this two-day conference while partaking in the litany of committees presented at COCMUN this spring. With topics ranging from online extremism within the political realm, the everchanging future of Russian-Ukrainian bonds, and an armed conflict fought in a galaxy far far away, this conference is promised to be the best one College of the Canyons has hosted yet. In closing, I would like to take a moment to express a huge thank you to all of our conference attendees for continuing to support our wonderful program, be our guest!

Kindest Regards,

Samantha Dalton, *Secretary-General*
COCMUN, Spring 2022
cocmodelun@gmail.com

Letter from the Under Secretary-General

To all Delegates,

Welcome to COCMUN 2022! After two long years, we can finally welcome all delegations back to the grounds of College of the Canyons to form part of our small, yet richly-developed conference; It is my distinct pleasure to serve as your Under-Secretary-General for the following two days.

Our exciting lineup of committees offers a host of topics that will be sure to light up the debate floor for the following days from the depraved depths of online crime, to the evolving Russia-Ukraine conflict, and finally, a civil war raging in a galaxy far, far away. There is no doubt in our mind that this weekend will serve as a platform for exciting discussions and solutions in our General Assembly and Specialized Body, as well as dramatic twists and turns in our crisis committee: Anything and everything can happen in the following days.

At its core, our Model UN program is built on emphasizing diplomacy and collaboration; Similarly, a key aspect of any conference is the relationships built among members of the committee as a way to resolve the issues presented to them. We strongly believe that our conference will be able to give our visiting delegates, as well as our staff, an opportunity to expand those connections and build those relationships through the highs and lows of the debate floor.

All the best and good luck,

Diego Staben, *Under-Secretary-General*
COCMUN, Spring 2022
cocmodelun@gmail.com

A Letter from the Chair

Honorable Delegates,

It is my pleasure to welcome you all to COCMUN 2022! It is my honor to staff such an amazing committee after being online for so long. My name is Amanda Marquez and I am ecstatic to announce that I will be your Chair for the General Assembly Committee! I am currently a freshman at College of the Canyons majoring in Political Science. The recent uprising of political and human rights movements that have emerged, has only strengthened my passion for politics.

Throughout my time as a delegate in Model United Nations, I've found it to be one of the most rewarding experiences. I know I will carry on the skills I have learned from MUN throughout the entirety of my career. The College of the Canyons MUN program stresses the importance of diplomacy and respect for all delegates. In this committee, I encourage all delegates to be collaborative and make connections with each other.

The purpose of the United Nations is to maintain peace and security within nations throughout the world, with respect to sovereignty. It is important to address these issues presented in committee with the underlying knowledge of the functions and role of each committee. In order to properly model this, it is important delegates approach the issues fairly. Nonetheless, I am excited to meet every delegate and explore all of the creative solutions delegates come up with. Please contact me if there are any further questions as I would love to hear from you guys and make lifelong connections. Once again, welcome to COCMUN 2022!

Best,

Amanda Marquez, *Chair*
INTERPOL Committee
generalassemblycocmun@gmail.com

A Letter from the Chair

Dear Fellow Delegates,

Welcome to COCMUN 2022! My name is Branden Bohrnsen, and I have the distinct honor of serving as your Co-Chair for the General Assembly. I am looking forward to these two days, where I hope to find cooperation, diplomacy, and delegates taking charge to debate a variety of ideas and propose detailed solutions to a selection of highly relevant topics.

I'm in my second semester here at College of the Canyons, and I intend on transferring this semester to major in Political Science and either Data Science or Economics. In my free time, I am a hobbyist game developer and classical pianist, and I am deeply interested in public economics and welfare policy research. Additionally, I am an officer in the Political Science Club, and have competed in DECA, FBLA, and YMCA Teens & Government, where I had the chance to meet many passionate students taking charge to build and showcase their skills, not unlike what we are sure to encounter at COCMUN.

I am excited to meet you all, and I can assure you I will be paying the utmost attention to delegates who have put in the work and contributed positively to the event. We're all here because we love this program, so let's work together, build connections, and leave this conference as better delegates than when we entered it.

Best Wishes,

Branden Bohrnsen, *Co-Chair*
INTERPOL Committee
generalassemblycocmun@gmail.com

Sensitivity Statement

Given the nature of the topics discussed in this committee, delegates will be faced with content that can be triggering and disturbing, including but not limited to racism, sexism, homophobia, drug abuse, and sexual abuse.

We understand that there will be some actions taken in committee that may be sensitive to some marginalized groups of people. In light of this, we ask that you stay considerate and aware of any possible insensitive behaviors or speech. **College of the Canyons does not and will not tolerate any form of hate speech in the vein of racism, sexism, homophobia, or any other type of speech rooted in malicious intent.** If delegates are found guilty of any of the aforementioned, they may face disciplinary action up to and including expulsion from the conference.

If delegates should have any issues with the topics being discussed within this committee please contact the Secretary-General as soon as possible so that we may address any questions or concerns delegates may have and/or allocate you to another committee.

Committee Specific Rules of Procedure

COCMUN's General Assembly Committee Specific Rules of Procedure can be found within COCMUN's Delegate Handbook located on our conference website.

INTERPOL

This International Criminal Police Organization, founded in 1923, is an intergovernmental organization that enables communications, provides access and data on crimes and criminals on an international level.

Boasting 195 member countries, INTERPOL connects police networks all across the globe to collaborate and enhance the procedure and prosecution of criminal cases. It is made up of a General Assembly, which meets once every year. The main points of communication between the Secretariat across all nations are through an INTERPOL National Central Bureau (NCB).

Because of the range of crime INTERPOL can cover, it divides into three programmes that address pressing matters: Counter-Terrorism, Emerging and Organized Crime, and Cybercrime: This committee will focus on the Cybercrime programme. Given the rise and implementation of the Internet into the daily lives of global citizens, it is crucial to keep a watchful eye on those who abuse its expansive availability for malicious purposes, that be to turn average citizens into radical extremists, or abuse concealed networks to enable the trade of illicit goods and services.

Like the General Assembly of the United Nations, INTERPOL does not have executive powers and cannot arrest or act without the approval of each country's national authorities. Additionally, as it is generally with crimes, delegates need to consider what the priority should be when it comes to addressing the issues presented to them: Should nations prioritize prevention, action, or reformation?

Topic A: The Globalization of Online Extremism

I. Key Terms

A. Radicalization: Per the United Nations Office of Drugs and Crime, "[...] Refers primarily to the process of indoctrination that often accompanies the transformation of recruits into individuals determined to act with violence based on extremist ideologies."[1]

B. Propaganda: Multimedia communications designed to convince a group or groups of people of a certain ideological stance through explanations, justifications, or calls to action on a specific cause. This can be video or audio files, presentations, articles, magazines, among other forms of media.

a. According to the United Nations Office of Drugs and Crime, what constitutes "terrorist" propaganda is a "subjective assessment"[2].

C. Stochastic Terrorism: Refers to a phenomenon where the constant dehumanizing or demonizing of a subject or group of people can lead to violence that is statistically likely, but cannot be easily predicted.[3]

D. Shitposting - The activity of posting provocative (Usually ironic and low quality) content on social media as a means to distract, minimize, or become inflammatory in a meaningful conversation.

E. Echo-Chambers: [In news and media] An environment in which somebody only encounters beliefs and opinions already similar to their own, with little to no alternative forms of thought.

II. Background Information

With its coming in the 1990s, the World Wide Web has become the prime source of communication across the globe. The widespread appeal and accessibility of the Internet has led its users to a diverse amount of streams of communication, communities, and ideologies. However, despite the revolutionary advent of this technology, an unfavorable side effect to the "age of information" is the deluge of equally

[1] *The Use of the Internet for Terrorist Purposes,* The United Nations Office of Drugs and Crime, https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/ebook_use_of_the_internet_for_terrorist_purposes.pdf
[2] Ibid, 1
[3] *Lone Wolf Attack,* Wikipedia, https://en.wikipedia.org/wiki/Lone_wolf_attack

accessible, radical content that has made violence bleed into the real world from the confines of online spaces.

The presence of radicals online is not new: It simply feels a lot more present today than it did in the past. Extremists have been using online spaces as their recruitment hubs since before the term "World Wide Web" was even coined. Traces can be found from all the way back to 1985, with the creation of a digital bulletin board for the "White Aryan Resistance" as a means to facilitate communication and recruitment tactics in the United States: This bulletin board was found in the communication network that preceded the internet as we know it.[4] Many others followed suit, including a surge of websites run by jihadist extremists in the mid-to-early 2000s, all with the intent to disseminate propaganda and to recruit.[5] Over the course of the 2000s and 2010s, extremists continued to expand their presence online, riding the wave of up-and-coming social media platforms, such as Twitter, Facebook, and YouTube, and other more fringe platforms (i.e. 4chan) as their direct form of engagement.

Twenty years later, the amount of websites hosting radical content has significantly grown. For instance, in light of the COVID-19 a, over 300,000 suspicious websites have been created, leading to a 600% increase in cyberattacks to hospitals and facilities working on coronavirus vaccines, according to Izumu Nakamitzu, United Nations Under-Secretary-General and High Representative for Disarmament Affair.[6]

The presence of the internet on political and societal discourse has accelerated the process of radicalization across the board. For one, activity online is often shrouded in anonymity, allowing people who wouldn't be able to join extremist causes to find their way into these radical movements. For instance, it is often considered unacceptable for

[4] *Hate Online: A Content Analysis of Extremist Internet Sites,* Analyses of Social Issues and Public Policy, Vol. 3, 2003, http://floodhelp.uno.edu/uploads/Content%20Analysis/Gertstenfeld.pdf
[5] *Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies*, International Journal of Conflict and Violence, 2020, https://www.ijcv.org/index.php/ijcv/article/view/3809/3868
[6] *75 for UN75: A Conversation on Rethinking Radicalization*, United Nations, https://www.un.org/en/academic-impact/75-un75-conversation-rethinking-radicalization

women linked to jihadist movements to meet with men who are also extremists, or join one of their groups; This is a different story once they're shielded by anonimity.[7]

Furthermore, by eliminating physical and geological barriers, leaders of radical movements have been able to reach far and wide to create vast networks of like-minded individuals. The interactivity of internet features — emails, chatrooms, social media — allows for creators of this propaganda and its consumers to be in relatively equal footing, with neither of them feeling like one is above the other. By blurring the lines between readership and authorship, those following extremist movements find it significantly easier to feel like they are a part of the larger movement, as opposed to passive observers of their chosen cause. Previous generations of sympathizers and terrorists encountered this barrier, given that their main means of communication for propaganda were found in pamphlets, newspapers, etc.[8]

Recruitment

Extremist propaganda and messaging is a mix of moral, political, religious, ideological, and social narratives, originating from grievances that are sometimes rooted in some form of reality, but are often mixed with made-up or hyperbolized concerns.[9] Delivered in varying forms of media, such as videos, images, and blog posts, the ultimate goal of these messages is to dehumanize each specific group's perceived enemy as much as possible, while simultaneously affirming the actions and beliefs of their users.

The United Nations Office on Drugs and Crime published a handbook on the recruitment for radical causes. In said handbook, they outline three different recruitment patterns employed by radical movements:

---

[7] *Radicalisation in the digital era The use of the internet in 15 cases of terrorism and extremism,* RAND Corporation, 2013, https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf
[8] *American Jihadist Terrorism: Combating a Complex Threat,* Bjelopera, Jerome P., Congressional Research Service, 2013, https://sgp.fas.org/crs/terror/R41416.pdf
[9] *Countering the Appeal of Extremism Online*, Institute for Strategic Dialogue, 2014, https://www.dhs.gov/sites/default/files/publications/Countering%20the%20Appeal%20of%20Extremism%20Online_1.pdf

1. "'The Net': violent extremist and terrorist groups disseminate undifferentiated propaganda, such as video clips or messages, to a target population deemed homogeneous and receptive to the propaganda;
2. "'The funnel': entails an incremental approach, to target specific individuals considered ready for recruitment, using psychological techniques to increase commitment and dedication. Even targeted children who resist complete recruitment may develop positive outlooks on the group's activities;
3. "'Infection': when the target population is difficult to reach, an 'agent' can be inserted to pursue recruitment from within, employing direct and personal appeals. The social bonds between the recruiter and the targets may be strengthened by appealing to grievances, such as marginalization or social frustration."[10]

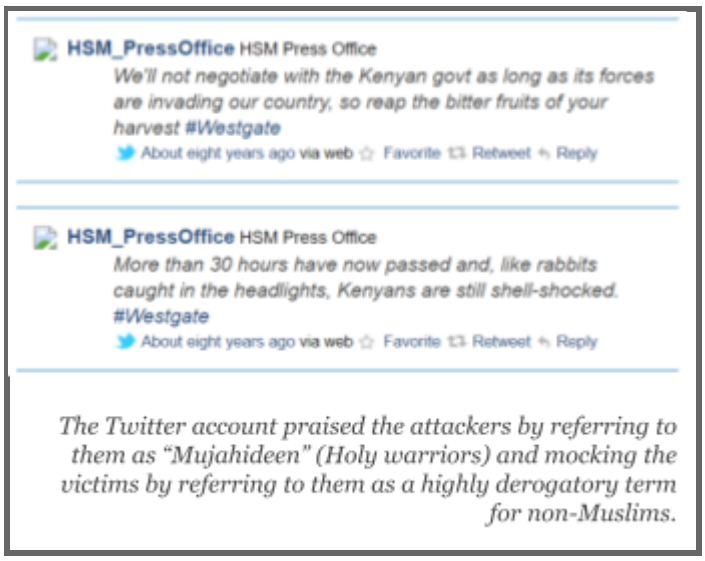
These patterns of recruitment begin with small forms of content that cater to a generalized view of a topic. Eventually, through algorithms designed to continually cater to the individual's likes and dislikes, the content inevitably veers towards extreme and harmful ideologies, driving away the original moderate intent. This phenomenon has also been labeled as "pipelines". Mainstream social media platforms such as Twitter, Facebook, and YouTube have become the primary means to catapult a user's fall into radicalization pipelines due to their accessibility. An example of this can be seen in an analysis of 72 million YouTube user comments, spread across 330,000 videos and 349 channels, showing that users consistently moved from milder to more extreme content, with most of the content catering to far-right ideology.[11]

In addition to serving as jumping-off points, social media services also function as a platform for extremists to boast about their "victories". This was the case in the

[10] *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System*, United Nations Office on Drugs and Crime, 2017, https://www.unodc.org/documents/terrorism/Publications/HB%20Children/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf

[11] *Radicalization pipelines: How targeted advertising on social media drives people to extremes*, The Conversation, 12 January 2022, https://theconversation.com/radicalization-pipelines-how-targeted-advertising-on-social-media-drives-people-to-extremes-173568

2013 al-Shabaab-led attacks on the Westgate Mall in Nairobi. Coming from the Somali-based organization with links to al-Qaeda, the attack was live-tweeted by leaders of al-Shabaab, praising the actions of the aggressors while utilizing incendiary rhetoric to convey their message.[12] Although Twitter eventually suspended the account, the damage was already done. [13]



The Twitter account praised the attackers by referring to them as "Mujahideen" (Holy warriors) and mocking the victims by referring to them as a highly derogatory term for non-Muslims.

The use of memes and "shitposting" is also a way in which many involved in radical movements hide their exploits behind the screen. While many radical groups are overt regarding their intentions, many others hide behind the use of jokes and irony. If policed about their beliefs, this practice allows these groups to quickly decry the infringement upon their individual rights to self-expression.

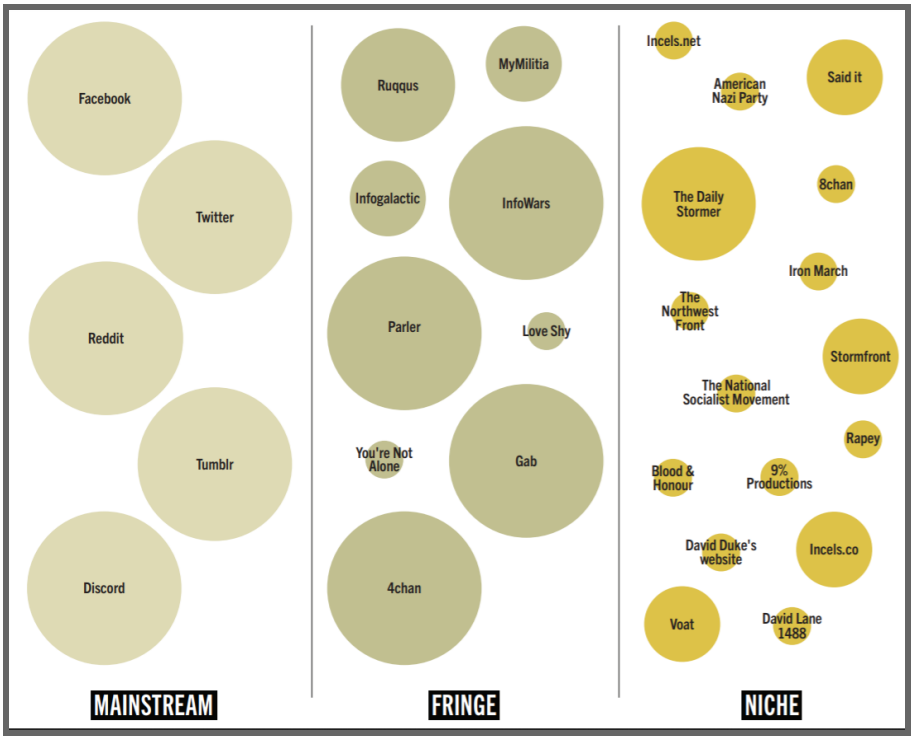
One of the most common rhetorical tactics used by recruiters is to appeal to the content consumer's sense of duty, creating a victim complex and simultaneously preying on the consumers' sense of identity and overall purpose. Recruiters tend to frame their cause around the idea that it is of utmost importance and amplify their calls to action as means to "do something."[14]

In addition to exposing users to their philosophies and ideologies, extremist groups often provide their users with a sense of community and belonging. These communities reinforce the already-held beliefs of those being radicalized and create echo-chambers where the users' perspectives are rarely challenged and are more often

[12] *Tweeting terrorism: How al Shabaab live blogged the Nairobi attacks,* The Telegraph, 22 September 2013, https://www.telegraph.co.uk/news/worldnews/africaandindianocean/kenya/10326863/Tweeting-terrorism-How-al-Shabaab-live-blogged-the-Nairobi-attacks.html
[13] Picture: Ibid, 12
[14] Ibid, 9

reinforced by others within that same community[15]. This further isolates the individuals into an ideological niche, where they constantly find themselves consuming information that satisfies and doesn't challenge their already-held beliefs[16]. This is especially true once a user has fallen deeper into a radicalization pipeline, where they have already gained access to more fringe and niche websites that exacerbate their already loud echo-chamber.

Factors Leading to Radicalization



According to former INTERPOL Secretary-General Ronald K. Noble, "The advent of the Internet has made the process of radicalization easier to achieve and the process of combating it that much more difficult, because many of the behaviors associated with it are not in and of themselves criminal," a fact compounded by the

[15] Ibid, 7
[16] *Segmenting the Electorate: The Effects of Exposure to Political Extremism Online*, 10 August 2010, https://www.tandfonline.com/doi/abs/10.1080/10510974.2010.497069

dramatic rise of extremist websites between 1998 and 2006, rising from 12 to over 4,500 sites in the span of eight years.[17] [18]

While there is no set path or specific attributes that can lead to radicalization, there are certain consistencies in the radicalization process that can eventually lead to terrorism. A study conducted by the National Institute of Justice sampled the backgrounds of both lone-actor and group-based extremists and found that, "having a criminal history, having mental health issues (or having received a diagnosis of schizophrenia or delusional disorder among lone actors), being unemployed, being single, being a loner or socially isolated, and having military experience were associated with a higher likelihood of engaging or attempting to engage in terrorism in research that included both group-based and lone-actor extremists, as well as in at least one study that included only lone-actor terrorists."[19] One of the outstanding risk factors the study concluded could inform a radicalized individual is social isolation. As mentioned previously, radical communities often bond over their ideology and online exploits. In seeking the validation that they lack in the real world as a result of their isolation, those drawn to radical ideologies can find this sense of community and friendship very valuable.[20]

Case Study: Christchurch

The Christchurch Mosque Shootings, perpetrated by a white nationalist in New Zealand, was the result of online rhetoric turning into stochastic terrorism.

Reports claim that the terrorist expressed far-right beliefs from a young age, using the message board 4chan from the young age of 14, and using the internet with

[17] *Preventing Internet radicalization of youth requires global police network, INTERPOL Chief tells police summit,* INTERPOL, 21 September 2010, https://www.interpol.int/en/News-and-Events/News/2010/Preventing-Internet-radicalization-of-youth-requires-global-police-network-INTERPOL-Chief-tells-police-summit.
[18] Picture: *The Online Extremist Ecosystem,* The RAND Corporation, https://www.rand.org/pubs/perspectives/PEA1458-1.html
[19] *Risk Factors and Indicators Associated With Radicalization to Terrorism in the United States: What Research Sponsored by the National Institute of Justice Tells Us*, U.S. Department of Justice, July 2018, https://www.ojp.gov/pdffiles1/nij/251789.pdf
[20] *Propaganda, Extremism and Online Recruitment Tactics*, Anti-Defamation League, https://www.adl.org/education/resources/tools-and-strategies/table-talk/propaganda-extremism-online-recruitment

little to no supervision before that.[21] The terrorist further revealed to investigators that he frequented message boards with far-right and extremist ideals, as well as using YouTube as source of inspiration for his eventual attack.

On the day of the attack, the terrorist emailed a 74-page manisfesto to authorities and media outlets, which included references to alt-right conspiracy theories and memes; The document was in turn propagated in the controversial message board 8chan.[22] Message boards like 4chan and 8chan, both of which thrive with extremist content due to their incredibly lax moderation policies, have been used as starting points for radicalization through content such as memes, and have also been used to publish manifestos similar to the one referenced above. In addition to this, the terrorist livestremaed the attack on Facebook, making references to memes, far-right conspiracy theories, and commonly-held beliefs and ideologies from far-right circles.

III. Past International Action

There is a lot of debate among scholars and policy-makers as to what constitutes "violent extremism," and the criteria that qualifies as such is spotty at best. Multiple studies employed for this document, had differing — albeit, close — definitions for what defined "radicalization" and "extremism". This is due to the fact that radicalization doesn't always lead to violence or connote harmful ideologies.

Regardless, one of INTERPOL's initiatives to prevent terrorism bred from online extremism is by the careful analysis of social media platforms to detect witnesses of attacks, as was the case in the London Bridge attack in the UK in 2017.[23] In addition to

[21] *Report finds lapses ahead of New Zealand mosque attack*, The Associated Press, https://apnews.com/article/intelligence-agencies-shootings-brenton-tarrant-new-zealand-new-zealand-mosque-attacks-d8217fa30fe4eeba45fb001b77857385
[22] *Jacinda Ardern's office received manifesto from Christchurch shooter minutes before attack*, ABC News, 16 March 2019, https://www.abc.net.au/news/2019-03-17/jacinda-ardern-christchurch-shooter-manifesto-email/10909874
[23] *Analyzing Social Media*, INTERPOL, https://www.interpol.int/en/Crimes/Terrorism/Analysing-social-media

this, INTERPOL has published a handbook — in conjunction with the UN — for online counter-terrorism operations. The handbook aims to provide resources to help investigators obtain and analyze information found online, specifically in social media, with the intent of enhancing counter-terrorism operations.[24] Additionally, the United Nations launched the International Hub on Behavioural Insights to Counter Terrorism, which, according to the head of the UN Office of Counter-Terrosim Vladimir Voronkov, "[...] Will help us understand why and how people become radicalized to violence and where we can intervene most effectively to halt the radicalization process."[25]

Furthermore, individual countries have adopted their own policies and commitments to combat online extremism and terrorism. New Zealand Prime Minister Jacinda Ardern, for instance, adopted the "Christchurch Call," in conjunction with French President Emmanuel Macron as a means to deter the consequences of online radicalism[26]. The Christchurch Call commits government and tech companies to develop tools to weed out online terrorism and radicalization, increasing transparency for content detection and removal, and reviewing algorithms that can direct users to extremist content.[27] In addition, individual states have adopted their own counter-terrorism strategies that address radicalization online, such as the UK's *Prevent* strategy, which outlines its own definiton of "radicalization".

Media Literacy has also been a focal point in action against online radicalism. The United Nations Educational, Scientific and Cultural Organization has recommended media literacy to be the most effective strategy in the way of preventing online

[24] *INTERPOL and UN publish joint handbook for online counter-terrorism investigations*, INTERPOL, 11 July 2019, https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-and-UN-publish-joint-handbook-for-online-counter-terrorism-investigations
[25] *New global hub to study factors driving radicalization and violent extremism*, United Nations, 7 December 2020, https://news.un.org/en/story/2020/12/1079432
[26] *New Zealand PM lauds Christchurch 'roadmap' to combat online extremism*, NBC News, 15 May 2019, https://www.nbcnews.com/video/new-zealand-pm-jacinta-ardern-lauds-christchurch-call-roadmap-to-combat-online-extremism-59692613948
[27] *Christchurch Call to eliminate terrorist and violent extremist online content adopted*, New Zealand Government, 16 May 2019, https://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted

radicalization and eventual terrorism.[28] This approach has become especially relevant when addressing the types of targeted content delivered by algorithms that gradually pull online users to either side of an online extremist group. According to the Report of the High-level Group of the Alliance of Civilizations, "Media literacy programs should be implemented in schools, particularly at the secondary level [...] to promote media awareness and development of Internet literacy to combat misperceptions, prejudices and hate speech."[29]

IV. Concluding Remarks

Online radicalization is — arguably — significantly more dangerous than past methods of radicalization due to the vast openness and generally unfiltered nature of the internet and online spaces. While most nations will agree on the importance of addressing and shutting down this issue, it will ultimately come down to which approaches should be prioritized to most effectively deal with the issue at hand.

In addition to this, many of those involved in extremist movements will perceive any actions to shut down their activities as an infringement of their individual privacy and self-expression, that be religious or personal beliefs. While there are legislative documents that rule speech that can lead to violence can be penalized, Delegates need to be aware of the tactics extremists use to disguise their content as inconsequential (i.e. "Shitposting").

Additionally, delegates need to be wary of their own norms and customs: What may be considered radical in one region, may be considered moderate or the standard in another. Furthermore, acts of terrorism are rare and sporadic. They can affect any region of the world, with equally tragic consequences, regardless of socio-economic

[28] *UNESCO addresses youth radicalization and online hate speech at Nice conference*, United Nations, https://www.un.org/youthenvoy/2017/02/unesco-addresses-youth-radicalization-online-hate-speech-nice-conference/
[29] *Media and Information Literacy as a Means of Preventing Violent Extremism,* UN Chronicle, https://www.un.org/en/chronicle/article/media-and-information-literacy-means-preventing-violent-extremism

standing on the global scale. However, extremist factions can be most prominently found in developing or war-torn nations. While extremist movements still exist within developed nations, they are much more well-hidden and less present on a day-to-day basis.

V. Bloc Positions

The general consensus on the proliferation of online extremism remains fairly universal at all points. However, member states need to be aware of their standing on the geopolitical scale and how that affects the progress of radicals in their own country. In the end, it is a matter of what the priority should be when addressing this topic: Should it be prevention? Or should it be immediate action?

Developed Countries

For the most part, countries with strong infrastructures and communication networks are not at immediate risk. However, these countries need to remain mindful and aware of the possibility of stochastic terrorism, as these are the countries where terrorist attacks are least expected to happen. For this reason, countries in this bloc need to prioritize prevention and focus on those at risk, and reform those that have fallen down the pipeline. Additionally, given that these countries have the resources to keep track of extremist movements within their own populations, this bloc needs to be extra vigilant about how these radicals conceal themselves and their activities.

Developing Countries

Developing countries find themselves being highly susceptible to not only violent attacks but also the constant threat of growing numbers within the ranks of extremist organizations. Countries in conflict or with larger radical presences, like Middle Eastern countries, are especially susceptible due to existing and established radical movements.

Delegates representing developing countries will need to focus on disrupting these movements head-on.

VI. Questions to Consider

1. Given the nebulous nature of some online behavior, how can nations track and prevent online radicalization while taking into account benign statements?
2. Should the priority of preventative measures lie on the prevention of further individual radicalization, or on the dismantling of larger online spaces that allow for the exposure of extremist ideas?
3. What measures can be taken to slow down the online growth of extremist organizations in nations that have not yet been largely impacted by radical terrorism?
4. How can nations work with the private sector and large social media corporations to combat the growth of extremism?
5. What can be done to rehabilitate those who have fallen down extremist pipelines?
6. Can nations find a concrete meaning and criteria to extremism, while acknowledging that what is considered “extreme” can vary among nations and cultures?

Topic B: Disrupting Criminal Activity on the Dark Web

I. Key Terms

A. Layers of the Internet:[30]

- **a. Surface Web:** Made up of publicly accessible pages of information that can be accessed through search engines and connected through each other using hyperlinks.
- **b. Deep Web:** Sections of the internet intentionally walled off from public view, and cannot be accessed through search engines.
  - i. E.g. Paywalls, email inboxes, intranets, banking services.
- **c. Dark Web -** Per RAND Corporation, "the portion of the internet that uses both encryption and anonymizing communication technologies, which are designed to promote anonymity and frustrate organized tracking efforts."

B. TOR: Short for "The Onion Router," a free and open-source software that enables anonymous communication; The most common tool used to access the dark web.

C. Cryptocurrency: A decentralized form of digital currency.

- **a. Altcoin:** Alternatives to Bitcoin.

D. Malware: Refers to any type of malicious software that is designed to exploit or harm any type of programmable device, network, or software.

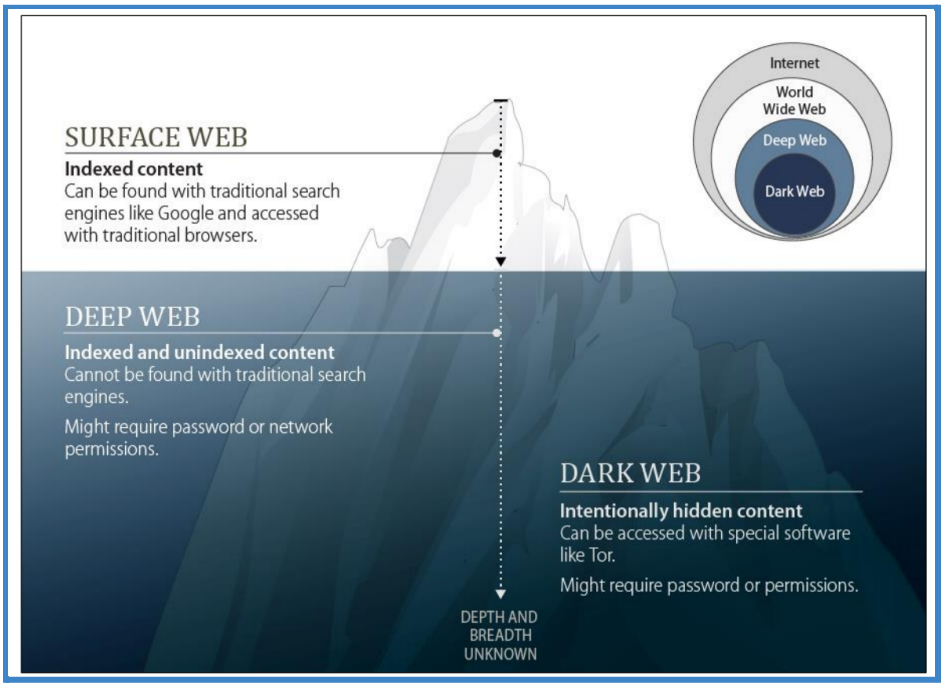
II. Background Information

On a day-to-day basis, the average user of the internet only sees one side of the expansive network, that being the surface web. However, while it might seem like the vast majority of the internet is the surface web, it really only makes up about 0.03% of

[30] *Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web,* RAND Corporation, https://www.rand.org/pubs/research_reports/RR2704.html

the World Wide Web.[31]The vast majority of the rest of the internet consists of the "deep web," 0.01% of which is the "dark web".

Developed by the U.S. Naval Research Laboratory to conceal online communications,[32] The dark web has since been widely known to host a multitude of illicit content as well as enabling the purchase and provision of illegal services, essentially making it the internet's black market.



The dark web has to be accessed through a number of networks, the commonly used one being TOR, short for The Onion Router; TOR was a tool developed by the Naval Academy in the 1990's with the goal of enabling the exchange of anonymous communications, and was released to the public in 2002[33]. TOR works by hiding the user's IP address and providing users with the most essential aspect of navigating the dark web: Complete anonymity. However, this is not the only network to look out for.

[31] *What's the Difference Between the Deep Web and the Dark Web?*, Encyclopedia Britannica, https://www.britannica.com/story/whats-the-difference-between-the-deep-web-and-the-dark-web
[32] *Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers*, SAGE Journal, https://journals.sagepub.com/doi/full/10.1177/0022018320952557
[33] *Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs*, National Institute of Justice, https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs

While it is the most commonly used, other anonymous networks have been used to enter the dark web, including I1P and Freenet.[34] [35]

A study conducted by researchers at King's College estimated that over 57% of the websites on the dark web are designed to facilitate criminal and illicit activity.[36] Though TOR estimates that about 1.5% of its users access these hidden services and pages[37], specific data on the usage of the network is lacking and difficult to collect due to the vast anonymity employed by users of the dark web. Furthermore, considering the types of crimes that are facilitated by users of the dark web, the lacking data cannot go unnoticed, as the crimes perpetrated in the dark web can go unpunished due to its untraceable nature. This network has been cited for facilitating crimes such as the trade of illicit goods, such as weapons, exotic animals, drugs, stolen goods and information such as Social Security Numbers and passwords. It has also been known to facilitate human trafficking, assassins for hire, and the enabling of the content relating to child abuse. A study conducted at the University of Portsmouth estimated that a disturbing 80% of illicit searches on the dark web related to pedophilia.[38] The total anonimity of the the dark web has also allowed for forums the enable the organization and execution of terrorist and criminal acts.

Despite the abhorrent uses the dark web has been known to form, it should be noted that the dark web is still utilized by actors who are not involved in any form of criminal activity. In fact, the dark web's original intent when developed by the Naval Academy was, "to conceal the identities of American operatives or dissidents attempting to communicate within oppressive regimes."[39] The anonymity enabled by the dark web has been known to be used not only by private citizens and businesses seeking privacy, especially those in countries with highly restrictive and oppressive governments that impose limited freedom of speech, but by government sectors as well. For example

[34] *Online African organized crime from surface to dark web,* INTERPOL, 2020
[35] Picture: *Dark Web,* Congressional Research Service, https://sgp.fas.org/crs/misc/R44101.pdf
[36] Ibid, 32
[37] Ibid, 35
[38] *The Dark Web Is Still A Huge, Difficult Problem*, Forbes, https://www.forbes.com/sites/timsparapani/2016/06/28/the-dark-web-is-still-a-huge-difficult-problem/?sh=30a8de3a65b1
[39] Ibid, 35

political dissidents in Egypt and Iran have used TOR to anonymize their movements in communications. Additionally, U.S. law enforcement organizations, such as the FBI, have used the network to develop malware to compromise servers and identify malicious users of TOR.[40]

III. Recent Developments

In recent years, a major factor in the trade of illicit goods and services on the dark web, along with other types of cybercrime, is the advent of cryptocurrency. The introduction of Bitcoin in 2009 eased transactions, as the untraceable form of cryptocurrencies exacerbated the anonymity already provided to those participating in criminal activity. While a record exists of the transactional movements of Bitcon and other cryptocurrencies, the actual source of the transaction is not recorded in any capacity. With the introduction of Bitcoin, there also came the rise of Altcoins, which further complicates the detection and tracing of actors using decentralized currencies to make purchases[41]. Furthermore, complicating this aspect of the issue is the exterior use of cryptocurrencies for non-criminal purposes.

Case Study: Silk Road

2011 saw the launch of the first dark web market: Silk Road. Founded and operated by "Dread Pirate Roberts," the pseudonym employed by the actual creator of the website, Ross Ulbricht. The website has become notorious for being the base model for what a black market in the dark web could look like:

> *"The Silk Road website, which has a customer-friendly electronic storefront that displayed bricks of cocaine as deftly as Amazon displays books, was the cyber-underworld's largest black market, with $1.2 billion*

[40] *Dark Web,* The Congressional Research Service, https://sgp.fas.org/crs/misc/R44101.pdf
[41] *INTERPOL holds first DarkNet and Cryptocurrencies Working Group*, INTERPOL, https://www.interpol.int/en/News-and-Events/News/2018/INTERPOL-holds-first-DarkNet-and-Cryptocurrencies-Working-Group

in sales and nearly a million customers. Beyond illegal drugs, the site served as a bazaar for fake passports, driver's licenses and other documents, as well as illegal service providers, such as hit men, forgers and computer hackers." - USA Today, 2013[42]

The website was particularly infamous for its aforementioned ease of use and its extensive provisions of illicit substances and materials, as well as services. Silk Road was mostly known for its extensive catalogue of drugs: Over 7,000 of the 10,000 listed items on the website were drugs.[43] In addition to that, the most common form of payment used by consumers on the Silk Road was Bitcoin. The DEA seized 11.02 bitcoins in June 2013, worth $814 cumulatively at that time.[44] Before being seized by the FBI, Silk Road boasted a total of 957,079 registered users.[45]

IV. Past International Action

Most of the actions taken by states and intergovernmental organizations to expose the criminals of the dark web have been through elaborate raids and working groups that address and research the issue extensively.

Operation DisrupTor was a successful attempt by multiple member states to disrupt the operation of Wall Street Market, the then second largest illegal market on the dark web. The operation was carried out in September 2020 by the European Union Agency for Law Enforcement Cooperation and led to 179 arrests of vendors engaging in

[42] *How FBI brought down cyber-underworld site Silk Road*, USA Today, https://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/

[43] *Silk Road: the online drug marketplace that officials seem powerless to stop,* The Guardian, https://www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace

[44] *Drug Enforcement Administration seizes 11 Bitcoins from alleged Silk Road dealer,* The Verge, https://www.theverge.com/2013/6/26/4468302/drug-enforcement-agency-seizes-11-bitcoins-in-south-carolina-bust-silk-road

[45] *FBI shuts down online drug market Silk Road*, CNN, https://money.cnn.com/2013/10/02/technology/silk-road-shut-down/index.html

the illicit trade of drugs and firearms on Wall Street Market.[46] The operation seized over 500 kilograms of drugs, 64 firearms and $6.5 million of both cash and virtual currencies, with arrests being carried out in the United States, Germany, the Netherlands, the United Kingdom, Austria and Sweden. The Operation was led by Dutch National Police, Europol and Eurojust, an agency of the European Union that deals with co-operation of criminal matters among member states.

Additionally, the closure of Silk Road on behalf of the FBI is an example of how individual states have acted against the illicit activity on the Dark Web. The FBI has detailed that to catch Ulbricht, they intercepted communications sent from his account, starting with tracking down an exchange of messages that recorded Ulbricht trying to hire someone to kill an anonymous user who extorted him. After Ulbricht was tracked down, the FBI was able to track down and arrest Ulbricht, seizing the website and Bitcoins, valued at approximately $3.5 million at that time. The FBI partnered with the International Revenue Service, the Drug Enforcement Administration and an investigative unit of the Department of Immigration and Customs Enforcement to see the operation through.[47]

On the other hand, INTERPOL launched Project ITANIUM in May 2017, with the aim of investigating the use of cryptocurrencies in underground market transactions. Ending in April 2020, the project resulted in the creation of services and forensic tools that can be used to monitor trends in dark web market ecosystems and analyze transactions across different virtual ledgers.[48] INTERPOL is also part of Project ENACT, which works to mitigate organized crime, including disrupting dark web operations, in Africa.[49] INTERPOL provides strategies, communication networks, and investigative

[46] *International sting against dark web vendors leads to 179 arrests*, EUROPOL, https://www.europol.europa.eu/media-press/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests
[47] Ibid, 44
[48] *Project Titanium*, INTERPOL, https://www.interpol.int/en/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Project-Titanium
[49] *Project ENACT,* INTERPOL, https://www.interpol.int/en/How-we-work/Criminal-intelligence-analysis/Project-ENACT

resources to police in Africa to aid in the fight against transnational crime in the region, a lot of which is facilitated by the dark web.

In a purely legislative sense, however, the dark web remains largely unnoticed. The most recent type of legislation aimed to disrupt criminal operations was proposed by Australian home affairs minister Peter Dutton. The bill gives Australian Federal Police and the Australian Intelligence Commission powers to disrupt and investigate a broader range of crimes with the creation of new types of warrants that directly tackle dark web operations.[50] According to Dutton, the bill takes aim at child abusers, terrorists, online arms traders, and human trafficking, among others.[51] Despite the extensive coverage of the bill, some critics have argued that the bill provides extraordinary powers to authorities with little oversight, creating potential privacy issues.

V. Bloc Positions

The act of finding and disrupting malicious actors on the dark web is complicated, primarily by the extent of certain jurisdictions across nations. The anonymity provided to users of hidden networks and services also makes them incredibly hard to keep track of in finding, an issue only exacerbated by the lacking data of what truly goes on the dark web, but more specifically what criminal actors do. It is also worth being noted that the dark web, while known in the public as the seedy underbelly of the world wide web, does have benefits to legitimate actors who are seeking privacy for one reason or another. Weeding out the ones who use anonymity for malicious purposes is key.

[50] *New powers to combat crime on the dark web*, Minister for Home Affairs (AU), https://minister.homeaffairs.gov.au/KarenAndrews/Pages/new-powers-to-combat-crime-on-the-dark-web.aspx
[51] *Dark web crime: how Australia's powerful new warrants would work,* The Guardian, https://www.theguardian.com/australia-news/2020/dec/03/dark-web-how-australias-powerful-new-warrants-would-work

Developed Countries

Developed Countries have expansive networks and law enforcement resources that can be used to track down and mitigate dark web and cybercrime operations. Despite this, those that are part of this bloc need to keep in mind that while a lot of the perpetrators of the dark web are foreign, the headquarters are usually located within their own countries. Furthermore, the stronger communication systems found within developed countries means there is a higher likelihood that hidden networks, such as TOR, can be accessed by those in this bloc (e.g. The vast majority of those captured in Operation DisrupTor were from larger developed countries like the United States).[52]

Developing Countries

Developing countries face two primary issues when it comes to dealing with actors in the dark web: Lack of resources in their law enforcement departments and being hot spots for illicit activity. INTERPOL has warned that African countries are at an especially high risk of cybercrime, due to the lacking policies to combat cybercrime in many African nations. This is only exacerbated by the aforementioned lacking law enforcement resources that are commonly found in developing nations, especially regarding technology required and needed to keep up with crimes perpetrated online and on the dark web.

VI. Questions to Consider

1. How can the integrity of the dark web be preserved for those who use it for legitimate purposes?
2. What steps can be taken to protect people at risk from becoming victims of the dark web?
3. How can current victims of online perpetrators be helped?

[52] Ibid, 48

4. Anonymity is one of the main components that make the dark web an attractive prospect to criminals. Can criminal operations be disrupted without being invasive to private citizens?
5. How can governments work with INTERPOL to implement effective solutions to the ongoing issues regarding the dark web?