Written Statement of Proposed Testimony

The Dynamic Terrorism Landscape and What it Means for America
Committee of Homeland Security
U.S. House of Representatives

Nicholas J. Rasmussen
Executive Director
The Global Internal Forum to Counter Terrorism (GIFCT)

February 2, 2022

Chairman Thompson, Ranking Member Katko, Members of the Committee. It is indeed a privilege for me to join you today for this important hearing. I am here today in my capacity as Executive Director of the Global Internet Forum to Counter Terrorism, known by its acronym of GIFCT. GIFCT is a 501(c)(3) organization with a membership of 18 technology companies and the mission to prevent terrorists and violent extremists from exploiting digital platforms.

But as some members may recall, this is not my first appearance before this Committee. During my tenure as Director of the National Counterterrorism Center (NCTC), I had the honor to appear before you several times along with other senior government officials as the committee addressed important issues of homeland security concern. It is a pleasure to be back here with you virtually and I especially want to thank former Chairman Mr. McCaul for the very positive and constructive relationship that the Committee had with NCTC during my years of government service, as well as the strong support he provided personally to me as the NCTC Director.

I am also pleased and honored to share the panel this morning with other distinguished experts and voices who work on the complex and challenging landscape of terrorism and violent extremism, both here in the United States and around the world. I deeply admire their expertise and I am eager to share my perspective from GIFCT with them and with the members of the Committee.

In my prepared testimony, I will cover three things this morning:

First, I will offer a quick sketch of the online threat landscape, as seen from our perspective at GIFCT, working with scholars and technology companies around the world.

Secondly, I will share with the Committee the various work streams that GIFCT is pursuing to counter what terrorists and violent extremists are doing in the online space and our ambition to generate even more impact in the years ahead; and

Thirdly, and lastly, I will speak to the specific way in which GIFCT is pursuing our mission and our agenda, as a multistakeholder forum committed to transparency and inclusivity across all of our work streams.

GIFCT is a tech-led initiative offering a unique multi-stakeholder setting to identify and solve the most important and complex global challenges at the intersection of terrorism and technology. GIFCT's mission is to prevent terrorists and violent extremists from exploiting digital platforms. We also firmly believe that respect for universal and fundamental human rights must be central to how we work to fulfill this mission. Our vision is a world in which the technology sector marshals its collective creativity and capacity to render terrorists and violent extremists ineffective online.

It is with this mission and vision that we bring together key stakeholders -- from industry, government, civil society, and academia -- to foster essential collaboration, deliver concrete progress, and facilitate information-sharing to counter terrorist and violent extremist activity online. While multistakeholder work does not always move at the desired pace and satisfy every individual or stakeholder community on every occasion, this approach does mean that we can bring all the actors and sectors who share a piece of this problem set together and pursue well-informed, collaborative progress. It is clear to me that the threat landscape we face today requires this whole of society approach to effectively address its online and offline dynamics.

This brings me to my first area of focus this morning, the threat landscape. Online terrorism and violent extremism are cross-platform and transnational by nature. No individual has just one app on their phone or their computer, nor uses only one type of online service, and bad actors are no different. The current threat landscape is growing more dynamic every day with an increasingly diverse array of violent extremist ideologies circulating in the online environment. We are not in a place where we have the luxury to focus on only one set of ideological actors who are exploiting the internet to advance their violent agenda. ISIS or Daesh continues to find ways to exploit the online environment to their benefit, as do white supremacist and/or neo-Nazi organizations across the globe, accelerationists, ethno-nationalists of various forms, and others who propagate violence-inducing conspiracy theories. And even as our attention is drawn to particular variants of violent extremism that may seem novel or new to some, like those tied to the Incel movement, terrorist groups with long histories of activity online continue to pose new challenges to both companies and to law enforcement authorities.

The violent extremists and terrorists that operate today in the online domain are often agile, adaptative and savvy. They increasingly understand where policy red lines have been drawn by mainstream platforms and at what point policy enforcement is likely to drive them off a particular platform or cause them to lose access. These extremist actors migrate readily from one platform to another depending on the purpose they are pursuing with online engagement. They know when to take particularly sensitive topics, such as operational coordination, off of more mainstream platforms and continue the engagement on more permissive platforms. In many cases, they prepare in advance for loss of access to a platform by having a bank of alternate accounts at the ready. None of this should surprise us, as terrorists and violent extremists have always adapted themselves to the tactics that intelligence and law enforcement professionals use to disrupt them. They operate in the same way when it comes to their use of modern technology and communication tools, and this poses a significant challenge to those charged with enforcing policies and terms of service.

Countering terrorism and violent extremism online requires a global and heterogenous response, a response that recognizes that services developed and intended to be used by good actors seeking to operate productively are also susceptible to abuse and exploitation by bad actors seeking to cause harm. Indeed, even as digital platforms empower people through tools to communicate, share information, run businesses and organize, the online environment that these platforms comprise inevitably provides those same empowering tools for use by terrorists and violent extremists. Technological innovation, over the course of history and through to today's discussion of digital platforms in 2022, unfortunately, can serve both as a force for good, and as a potential accelerant to radicalization and mobilization to violence. That is the unfortunate reality that we confront.

The second set of comments I wanted to offer today relates to what GIFCT is doing in response to this threat picture and landscape. It is with this understanding of the challenges and threats we face today that GIFCT has set its strategic priorities, two of which I will highlight here this morning.

The first key priority for GIFCT this year is to recruit and welcome into GIFCT new member companies from around the world that represent different kinds of technologies. If the work of our organization is focused exclusively on social media platforms or on companies based in Silicon Valley, we will have failed to realize GIFCT's full potential and we will fall short of achieving the impact that we seek. The effort must extend globally and must involve companies and technologies of all sorts.

A second pressing priority guiding our work at GIFCT is to provide greater thought leadership on the issues and challenges associated with online terrorist and violent extremist activity. We do this in order to support our member companies as they develop their own solutions for content moderation and illicit user activity that fall within their own policies and terms of service. Focused on online content and behavior tied to offline violence, we are taking steps this year to develop a more useful definitional framework for identifying terrorist and violent extremist activity online that GIFCT member companies can draw upon to inform their ongoing efforts to monitor, assess, and take action against content and activity that violates their policies.

Both of these objectives — growing the scale and diversity of technology platforms committed to our mission and providing forward looking thought leadership that our members can leverage to address the corpus of activity they confront on their platforms — reflect, in part, our role in addressing the online factors and behaviors that shape today's challenging threat landscape. But it is imperative that I emphasize that ignoring the offline factors that contribute to that same landscape will not take us very far. It is neither strategically sound nor intellectually honest to view the online and offline threat landscapes as separate and distinct entities. The online ecosystem can only play the role of facilitating greater communication, information-sharing, and organizing for terrorism and violent extremism when other factors that contribute to this threat are present as well. Online consumption and exchange of information can surely be pointed to as an accelerating factor to the process of radicalization. Yet it is also clear that information drawn from other sources, including broadcast news outlets and rhetoric employed by political leaders and public figures, also plays a role in that pathway to extremist behavior.

A pressing example of this interplay between the online and offline space is the ongoing COVID-19 pandemic. The pandemic created a set of conditions that seems almost tailor-made for violent extremists seeking to advance their work. Between health restrictions, economic impacts, social isolation, and increased political polarization, it is clear that the pandemic has exacerbated existing cleavages and anxieties across society. While many throughout the pandemic and its lock downs have found solace and positive community through online engagements, other groups, smaller in size or number but higher in terms of risk, also use online communities to perpetuate misinformation and coordinate hate-based violence.

One consequence of this environment is increasing engagement and interaction online among individuals who otherwise may adhere to distinct and separate ideologies. Experts in our GIFCT academic network, the Global Network on Extremism and Technology, continue to see such online behavior and their conclusions very much align with and reinforce the insights offered by my fellow witness Dr. Miller-Idriss and others who have pointed to a post-organizational transformation within the threat landscape and to new coalition building as a result of disparate individuals and groups finding unity in their understanding of major world events and in their preferred solutions to societal problems.

It is with this clear-eyed understanding of today's current counterterrorism challenges and threat landscape that I chose to accept my role as the inaugural Executive Director of the Global Internet Forum to Counter Terrorism. Having served as long as I had inside government, it was clear to me that government alone could not solve those challenges and manage that threat landscape in a way that would keep us all safe from terrorists and violent extremists.

The current organization that is GIFCT, an independent non-profit organization, is less than two-years old but has been able to take the early progress of its original establishment as a consortium of technology companies to make meaningful contributions to addressing the online threat landscape. GIFCT was originally founded in 2017 by Microsoft, Twitter, Facebook, and YouTube, who then announced at the United Nations General Assembly in 2019 that the consortium would evolve into an independent organization. During the three years as a consortium, in-house teams at GIFCT's member companies initially focused on developing cross-platform tools such as the hash-sharing database and establishing a forum where technology companies, governments, academia, and civil society could discuss the state of the online threat landscape, share insights, and produce solutions. During this time, GIFCT's original membership criteria was established, our ongoing mentorship program with Tech Against Terrorism was created, the first phase of a GIFCT-funded academic network was launched, and GIFCT's first counterspeech campaign toolkit for practitioners in partnership with the Institute for Strategic Dialogue was created. After this initial progress, the transition to an independent non-profit organization was pursued so that GIFCT could achieve more impact for its member companies and do more to support efforts to fulfill the nine-point action plan signed by technology companies in the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online.

Today, GIFCT is a young and growing non-profit organization run by its own team of counterterrorism and technology experts. Working with our 18 technology company members, we embrace the task of moving the industry forward on how to address threats posed by terrorism and violent extremism and arm our members with cross-platform tools, solutions, and resources to: prevent further exploitation of their platforms; strengthen how companies respond to terrorist and mass violent attacks; and learn about new evolutions in the threat landscape and approaches to combating them.

We do this work with a full commitment to remain diligent in upholding the human rights and fundamental freedoms that terrorists so often seek to undermine. We believe that counterterrorism and human rights must be complementary and mutually reinforcing goals. Preventing terrorists and violent extremists from exploiting digital platforms enhances the protection, fulfillment, and realization of human rights. But this requires ongoing work to address and understand the human dimension and impacts of our efforts with a focus on both the victims of terrorism and violent extremism as well as those victims of efforts to address terrorism and violent extremism. Even in the short time GIFCT has been operating we have delivered real action to meet this commitment, commissioning a non-profit entity called BSR (Business for Social Responsibility) to conduct a human rights impact assessment of the organization that now serves as a guide for all aspects of our work from engaging stakeholders and technology companies across the globe, to the tools and resources we develop.

At GIFCT we continue to pursue development of cross-platform tools, such as the GIFCT hash-sharing database, so that a range of different digital platforms can take information on known terrorist and violent extremist content and activity and identify whether the same content exists and requires action on their respective platform. GIFCT's database is the safe and secure industry database of "perceptual hashes" - often understood as "a digital fingerprint" - of known terrorist content as defined by GIFCT's hash-sharing database taxonomy. Content found by a member company is "hashed" ensuring there is no link to any data from the original platform or user, including personally identifiable information. Hashes appear as digital signatures or numerical representations of the original content, which means they cannot be easily reverse engineered to recreate the content. Each company that is part of the hash-sharing database determines its use of and engagement with the database, depending on their own terms of service, how their platform operates, and how the threat of terrorist and violent extremist exploitation may manifest for them.

This work also requires refined parameters and a definitional framework for what constitutes terrorist and violent extremist content. With multistakeholder input, we provide members with thought leadership and resources as we continue to develop our taxonomy to address a more diverse range of terrorist narratives and ideologies while avoiding the use of overly broad definitions that pose risks of over-censorship. This is why hashes of terrorist and violent extremist content that qualify for the hash-sharing database must meet a taxonomy that recognizes the original producers of the content as well as the type of content and severity for harm.

Currently, our taxonomy addresses videos and images produced by individuals and entities on the United Nations Security Council's consolidated sanctions list as well as perpetrator-produced content captured or livestreamed during an offline violent attack. Material that meets these criteria is subject to hashing and sharing within the GIFCT framework. In the coming months, the taxonomy will expand to include attacker manifestos in PDF form, terrorist and violent extremist publications in PDF form, and URLs identified by our partner Tech Against Terrorism and confirmed to link to terrorist content. Member companies are then able to see if any hash may match to content on their platform, thus providing a signal to identify where to focus and prioritize their policy enforcement efforts and combat potential terrorist and violent extremist activity on their platforms.

To give an example of how the hash-sharing database operates, when a member company may identify a video produced by an entity on the United Nations Security Council's consolidated sanctions list that glorifies and celebrates a previous terrorist attack, that member can create a hash of the video – the digital fingerprint of the content that does not contain user data – and share it in GIFCT's database. This hash is now available to the other members of the GIFCT hash-sharing database who can then determine if the hash matches to content on their respective platforms, thus identifying if the video has been shared on their platform. If that is the case, the member can review the video and the context it was shared within to determine what actions to take in line with their policies and terms of service. Such a cross-platform tool enables our members to share and leverage each other's ongoing efforts and expertise and increase our collective impact to prevent the further exploitation of digital platforms when this video is shared. This is an important part of our work to support our member companies on an ongoing basis, as well as during the especially urgent instances in which a digital platform is being exploited as part of an offline violent attack.

A second critical mission for GIFCT is to improve the capacity of member companies to respond in a real-world terrorism crisis that may be playing out in the online environment. Through our Incident Response Framework, we facilitate situational-awareness and information-sharing across our members in real-time during an offline violent event in order to identify any online dimensions. In the event of a significant online dimension to the offline attack, the framework serves to strengthen the ability for our members to take swift action against online content produced by the perpetrators as part of their violence.

Since initially establishing this framework in the Spring of 2019, we have continued to mature and develop it in partnership with our members. To date, GIFCT and its member companies have initiated communications in response to over 195 offline violent events across the globe in as close to real-time as possible sharing situational awareness and information in an effort to identify any online dimension. In that time, the highest level of our Incident Response Framework, the Content Incident Protocol (CIP), has been activated twice in response to the perpetrators livestreaming their attacks and the content being shared on a GIFCT member platform. When the Content Incident Protocol is activated, GIFCT members can contribute hashes of the perpetrator-produced content to the GIFCT hash-sharing database in order to support all members in identifying the content on their platforms and taking action in line with their respective policies and terms of service.

The multistakeholder nature of our work is best highlighted through the thematic GIFCT Working Groups we convene to focus on specific challenges we see in our efforts to counter terrorism and violent extremism online. GIFCT Working Groups bring together experts from diverse stakeholder groups, geographies, and disciplines to collaborate and produce output with practical value and utility on an annual basis. This output is published on our website and is available to all. GIFCT Working Groups are refreshed each year with updated themes and focus areas with the opportunity for new participants to join and new problems to be addressed. GIFCT's 2021 Working Groups convened more than 200 experts and practitioners from across the world, holding more than 55 meetings with representatives from 10 technology companies, 13 governments and international governing bodies, 26 civil society organizations, and 41 research and academic institutions.

GIFCT's 2022 Working Groups are currently convening on a monthly basis with participants from 35 countries across six continents, with 57% drawn from civil society, academia or practitioners, 26% representing governments, and 17% from industry. These groups have been meeting since August 2021 and are currently pursuing substantive projects on key challenges to countering terrorism and violent extremism online focused on: technical approaches including tooling, algorithms and artificial intelligence; best practices and implementation hurdles for transparency; crisis response protocols; positive interventions and strategic communications online to support disengagement and intervention campaigns; and assessing legal frameworks. Last year's outputs from GIFCT Working Groups provided proof of concept that through multistakeholderism, we can achieve substantive results that offer practical analysis and well-informed recommendations on where tech and other sectors, often including GIFCT itself, can improve and the direction to take next.

I hope this brief summary gives Committee members and staff some idea of the substantive work underway at GIFCT and the various initiatives we are pursuing to limit the ability of terrorists and violent extremists to operate successfully in the online environment. That is the "what" of GIFCT's work and I am extremely proud of that work. In my view, however, the manner in which our work is carried out is equally important. How we do our work matters as much as what we do. That is the third and final thought I want to leave with you today.

Several times in the course of this statement for the record, I have referred to GIFCT's work as being multistakeholder. I would argue that this attribute is in fact what makes GIFCT unique and in many ways, an experiment. There are very few venues or fora, if any, that offer the sort of multistakeholder platform for problem solving and information sharing that we are working to build. It is a forum in which the full set of relevant stakeholders is invited to participate. And we have appreciated having representation from the United States government and from federal law enforcement within our Working Groups and on our Independent Advisory Committee.

As I left government service a few years ago, it was clear to me that more and more of the work necessary to deal with our terrorism and extremism challenges needed to take place outside of government, rather than within government. That meant collaboration and cooperation with the private sector, including technology companies, engagement with academics who understand how information and technology are used to radicalize individuals, and dialogue with civil society organizations that care deeply about the free and open circulation of information and ideas in a context of full respect for the rights of others. Solving our terrorism problems, and particularly our domestic terrorism problems, requires a whole of society approach – not just a whole of government approach – and I was eager to join the effort from outside government to try and make some real gains in this area. What was lacking was any sort of venue for helping organize and drive key work streams involving all of these different stakeholders.

GIFCT offers us that opportunity. The chance to bring together industry, government, civil society, and academia in common cause to make the online environment safer and healthier. That is what my colleagues and I at GIFCT are working every day to do. I would be the first to tell you that a tremendous amount of work to achieve that objective lies ahead of us and that much more remains to be done for us to realize the potential embodied in multistakeholder engagement of this kind. We are not yet fully there. But there is real urgency to what we are all here talking about today, because the threat environment we are all confronting is only growing more challenging and more dynamic every day. With the continued support of this Committee, and that of other critical stakeholders here in the United States and around the world, I am optimistic that we can continue to deliver genuine multistakeholder progress that makes the online environment a safer and healthier place. Thank you for your attention this morning and I look forward to your questions.