Reprisal Hacktivism Targets Indian Ideology

Published: 2023-04-28 · Archived: 2026-04-05 17:21:37 UTC

CRIL charts the evolution of recent Hacktivism targeting India, as well as reprisal attacks against the same.

An Internal Situation of Parallax & Disarray

Hacktivism has begun to pose a considerable threat to India due to its unique societal, ideological, and economic position in the continent.

The ongoing commotion, OpIndia/OpIndia 2.0, by several hacktivists and the response of pro-Indian hacktivists has escalated the situation, with businesses and governments caught in the middle of Peter Panners.

It is essential to understand the root cause of such campaigns that are incited due to negative sentiments promulgated through campaign words like ‘Islamophobia_in_India’ and ‘SaveIndianMuslims’ from within the country. The native/non-native and ideologically misled netizens often post fake content on social media that incite such hacktivist groups to misconstrue the actual socio-political conditions of a country and react.

Amidst such geo-political developments, Cyble Research & Intelligence Labs (CRIL) maintains a hawk-eyed approach to their impact on cyberspace. In the same stride, CRIL captures the account of associated hacktivist incidents affecting India and other countries in Asia.

Chronology of Hacktivist Campaigns Targeting India

In 2020, the farmer’s protest in India led to the emergence of hacktivist groups such as Anonymous India and the Red Rabbit Team. These groups use social media platforms to raise awareness about the protests and their

demands and carry out cyber-attacks against companies and individuals who were perceived to be against these movements.

Last year we observed a flurry of hacktivist incidents targeting India in a two-month-long campaign incited due to an internal political situation. These campaigns were initiated by a prominent hacktivist group **DragonForce** under the campaign **OpsPatuk** and were widely participated by several hacktivists sharing the same ideology. The same campaign progressed under OpIndia after DragonForce distanced itself from the campaign in June 2022.

OpIndia Reinstated by Team_insane_pk in 2023

Intermittent hacktivism incidents against Indian entities continued throughout 2022. After a brief lull, **Team_insane_pk** reinstated the OpIndia campaign on February 5, 2023, on Kashmir Solidarity Day, by launching DDoS attacks and leaked documents of the Indian government and private entities. Since then, the group has collaborated with several other hacktivists aligned against India.

Team_insane_pk is operated by a team of threat actors (TA); two of them were identified as **Mr Insane** and **HOAX1337**. The groups were also parallelly involved in targeting other counties, including the Philippines, Sweden, Afghanistan, Russia, Dominican Republic, Indonesia, and Brazil. Ironically, in the past, the group has also targeted Pakistan Government websites, such as *radio.gov.pk* and *pabalochistan.gov.pk*, claiming religious reasons to justify the attack.

Operation Payback

In 2023, another campaign was initiated in March under the name ‘Operation Payback’ by the hacktivist group **Mysterious Team Bangladesh**. The group launched numerous DDoS attacks against various Indian websites and publicized them over social media and internet messaging channels.

This campaign against India by Mysterious Team Bangladesh and other hacktivists was part of a previous global campaign in retaliation to the Indian sympathetic hacktivists targeting websites in Pakistan, Bangladesh, Indonesia, and Malaysia.

The group also leaked files from historical breaches and shared PDF, SQL, TXT, and image files stolen from various institutions. The files included various identification documents, including Aadhaar cards, PAN cards, passports, old bank statements, invoices, cheque books, and scanned payment cards. Most of the shared documents appeared outdated, while some remained valid according to their expiry date.

Mysterious Team Bangladesh has also historically been trying to run its hacktivism campaigns with a pro-Islamic ideology against several nations. The group claims to be active since 2012. However, they were actively involved in the May 2022 OpIndia/OpsPatuk campaign and the OpIsrael campaign targeting Israel.

Other hacktivist groups that supported this campaign were:

Mysterious Team Bangladesh	Ganosec Team
Team Insane PK	Hacktivist of Garuda
Khalifah Cyber Crew	Eagle Cyber Crew

OpsjentikRamadhan

Further, in the month of Ramadan, on March 27, 2023, another hacktivist group **EAGLE CYBER CREW** along with other 8 groups allegedly from Malaysia, Bangladesh, Pakistan, Indonesia, Yemen, Vietnam, Sudan, and Palestine, launched **#opsjentikRamadhan**.

These prejudiced groups, operating under the notion that Indian Muslims are victims of social injustice, carried out several DDoS attacks on the Indian side. During the same time, these groups were also involved in OpIsrael.

EAGLE CYBER CREW created its Telegram channel on December 2, 2022, and stated that it is of Malaysian origin. The hacktivist was also quite vocal in stating themselves as part of the ‘Army of Mahdi’ (*Mahdi refers to the prophesied redeemer of Islam who will appear before the end of the world to rid the world of evil and injustice in Islamic scripture*) and ‘Anti Dajjal Community’ (*Dajjal is an evil figure in Islamic eschatology*).

Assalamualaikum w.b.t and Salam Ramadhan to all Muslim's hacker.

We from EAGLE CYBER CREW (Malaysia) and from Team 8 United Nations, namely Bangladesh, Pakistan, Indonesia, Yemen, Vietnam ,Palestine (Insha'Allah Sudan and Rusia is coming too would like to launch #opsjentikramadhan during ramadhan the sacred month for all muslims.

This attack is aimed at responding to the actions of a group of Script Kid's Hacker 2023 originating from India who spread Muslims data in public. Other than India,we would like to attack Israel too.They still don't stop in attacking Palestinians as it is during the month of Ramadan that they will try to attack more severely.

‼️Stay Tuned Guys‼️

#opsjentikRamadan

Figure 1: Announcement of the campaign on the Telegram channel

The following affiliates participated in the campaign:

4 EXPLOITATION Channel	SynixCyberCrimeArmyMY
STUCX TEAM	TIGERCYBERTEAM
Mysterious Team Bangladesh	1915 TEAM
Team_Insane_pk official	KEP TEAM
PAKISTAN CYBER HUNTER	Mysterious Silent Force
T.Y.G Team	Ganosec Team

During the campaign, the EAGLE CYBER CREW group claimed to compromise the public-facing web infrastructure of the Punjab Police, India. Based on the posts, they leveraged a Local File Inclusion (LFI) vulnerability to gain access and leak internal configuration files from various sub-domains of the ‘punjabpolice.gov.in’. This also led to the disclosure of MySQL configuration files containing the usernames and

passwords of database users. This further led to the disclosure of access to the other backend files from different provincial websites of the Punjab Police Department.

Besides their campaign, the group, while coordinating with pro-Bangladesh group 'Mysterious Silent Force', launched DDoS attacks on several Indian banks public and private sector banks on April 27, 2023.

Anti-India Campaign by 'Anonymous Sudan'

'**Anonymous Sudan'** is a politically motivated hacktivist group active on their Telegram channel since January 18, 2023. Their activities began on January 23, 2023, with DDoS attacks on organizations in Sweden, Denmark, the Netherlands, France, Australia, and Israel. In April 2023, the group declared India their latest target to sympathize with Indian Muslims under their misperceived Islamic cause.

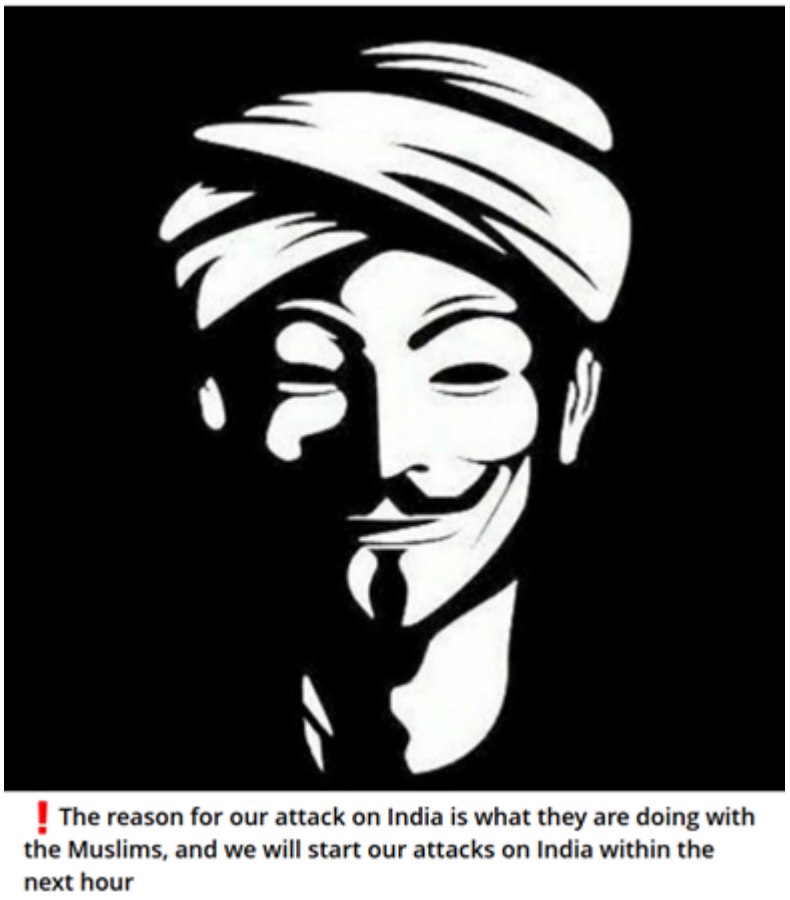


Figure 2: Announcement by Anonymous Sudan group on their Telegram channel

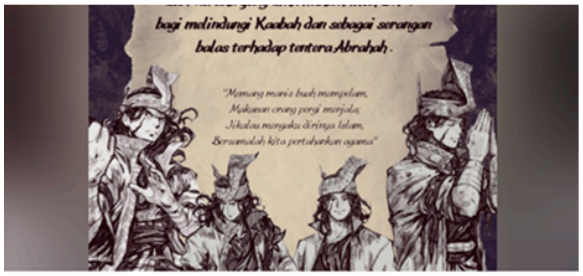
On their Telegram channel, the group "Anonymous Sudan" claimed to target websites of the Airports Authority of India (aai.aero), Delhi Airport, Mumbai Airport, Hyderabad Airport, Goa International Airport, and Cochin Airport. Other than these, the actors also targeted websites of healthcare institutions, including KIMS hospitals and Apollo Hospitals, to name a few. The TA shared connection status, apparently demonstrating successful Denial of Service on the websites.

OpsAbabeel:

On April 19, 2023, **EAGLE CYBER CREW** initiated a parallel campaign – OpAbabeel (*freedom from sadness, fears, and horrors)*, in collaboration with hacktivist groups, **4-EXPLOITATION**, **KHALIFAH CYBER CREW,** and **TIGER CYBER CREW**.

The ongoing campaign is in retaliation to Indian hacktivists leaking data of Muslim citizens. The campaign also garnered interest from Team_insane_pk officials and ISLAMIC CYBER CORPS. In this campaign, they used tactics like DDoS attacks, defacement, and selling compromised databases from India. However, the Indian data samples shared by these groups on their channel were from a 2020 leak from a threat actor active on the now-defunct BreachForum.

In this campaign, these groups primarily target Indian Government entities, the Judiciary, and Educational institutes. These groups are simultaneously also targeting companies in Mexico, the United States, Ghana, and Cyprus.



Assalamualaikum to All , We 4 EXPLOITATION Will Organize an Ops as response to Indian Government that want to attack and counquer Kaabah and as Response to other Indian Cyber Team That Insulted Our Religion

With much pleasure We invite All Muslim Hacker, Hacktivist, and all Freedom Fighter around the world to join us on Attacking Indian.

With much pleasure We invite All Muslim Hacker, Hacktivist, and all Freedom Fighter around the world to join us on Attacking Indian.

Memang manis buah mempelam
Makanan orang pergi menjala
Jikalau mengaku dirinya islam
Bersamalah kita pertahan agama

If you are True Muslim let's join us on this war.

#OpsAbabeel Engaged !!
@OpsAbabeel

#ECC
#EagleCyberCrew
#4-EXPLOITATION
#KhalifahCyberCrew
#TigerCyberTeam

Figure 3: Announcement of the campaign on the Telegram channel

OpIndia 2.0

OpIndia2.0 campaign was initiated at the behest of Indonesian hacktivist groups – **VulzSec** and **Hacktivist of Garuda** on April 20, 2023, in retaliation to the ongoing attacks on Indonesian government sites by Indian-sympathizing threat actors. The group claimed to launch DDoS attacks on 54 entities, primarily government websites of various states of India.

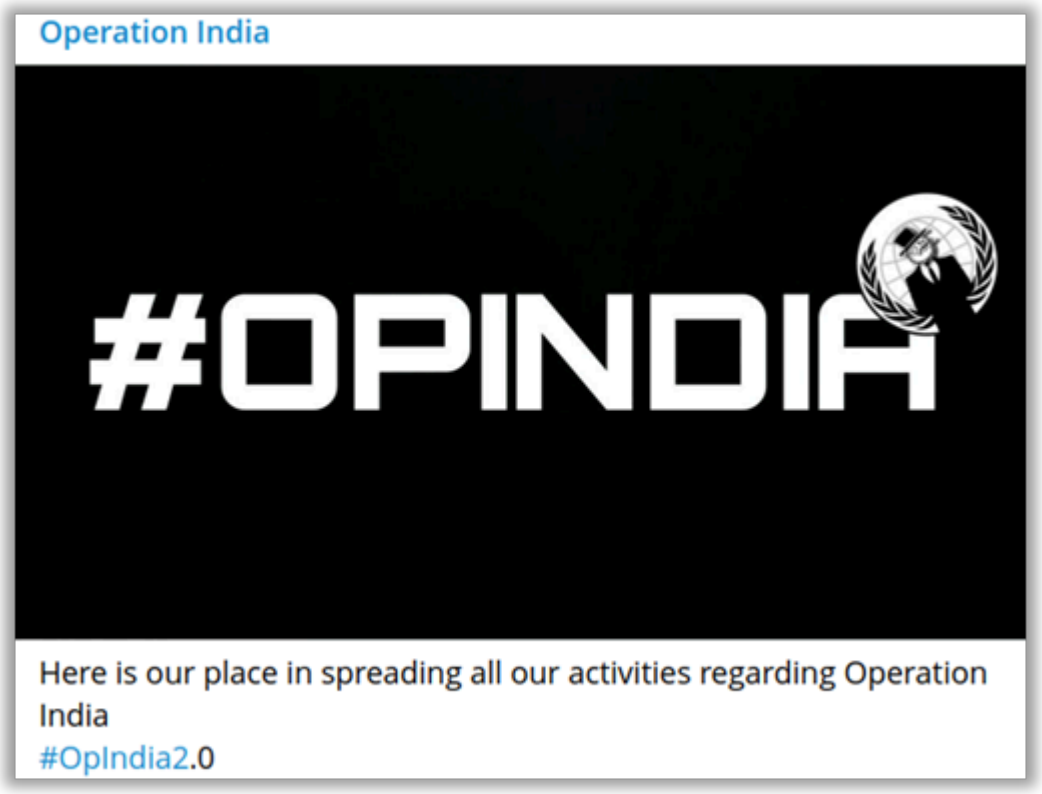


Figure 4: Announcement of the campaign by Hacktivist of Garuda

On April 26, 2023, VulzSecTeam declared to cease the OpIndia 2.0 campaign, when a pro-Indian hacktivist group, Kerala Cyber Xtractors, approached them. According to the conversation between the two, this campaign was also a result of misconceived notions about the perceived suffering of Indian Muslims.

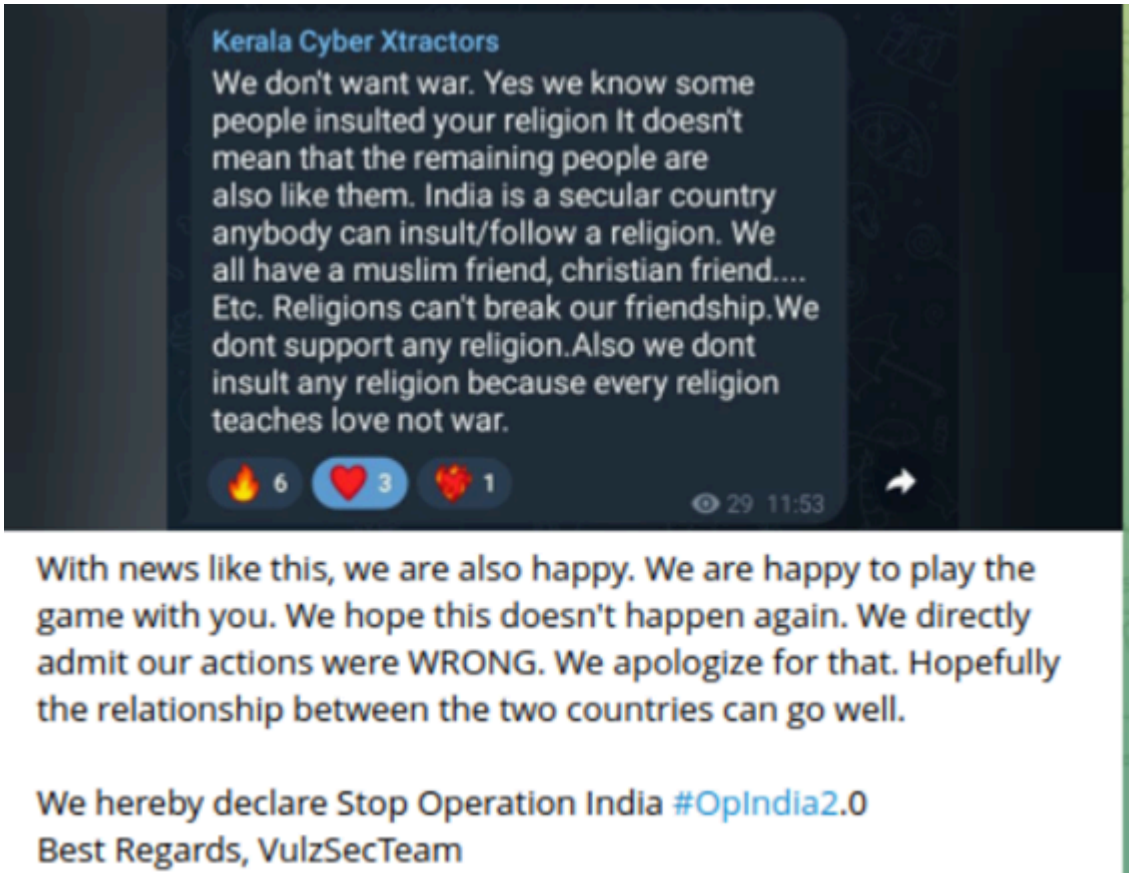


Figure 5: Excerpt from VulzSec Telegram channel, declaring to cease the OpIndia campaign.

However, other **Hacktivist groups such as GANOSEC TEAM and Team_insane_pk ignored this truce and continued their attacks on Indian cyber infrastructure.**

OpIndia23

Pro-Islamic groups came together to launch another campaign, **#OpIndia23,** on April 26, 2023. This is an ongoing campaign to protest against the perceived injustice and prejudice against Indian Muslims. This campaign was started after the conclusion of the OpIndia2.0 campaign.

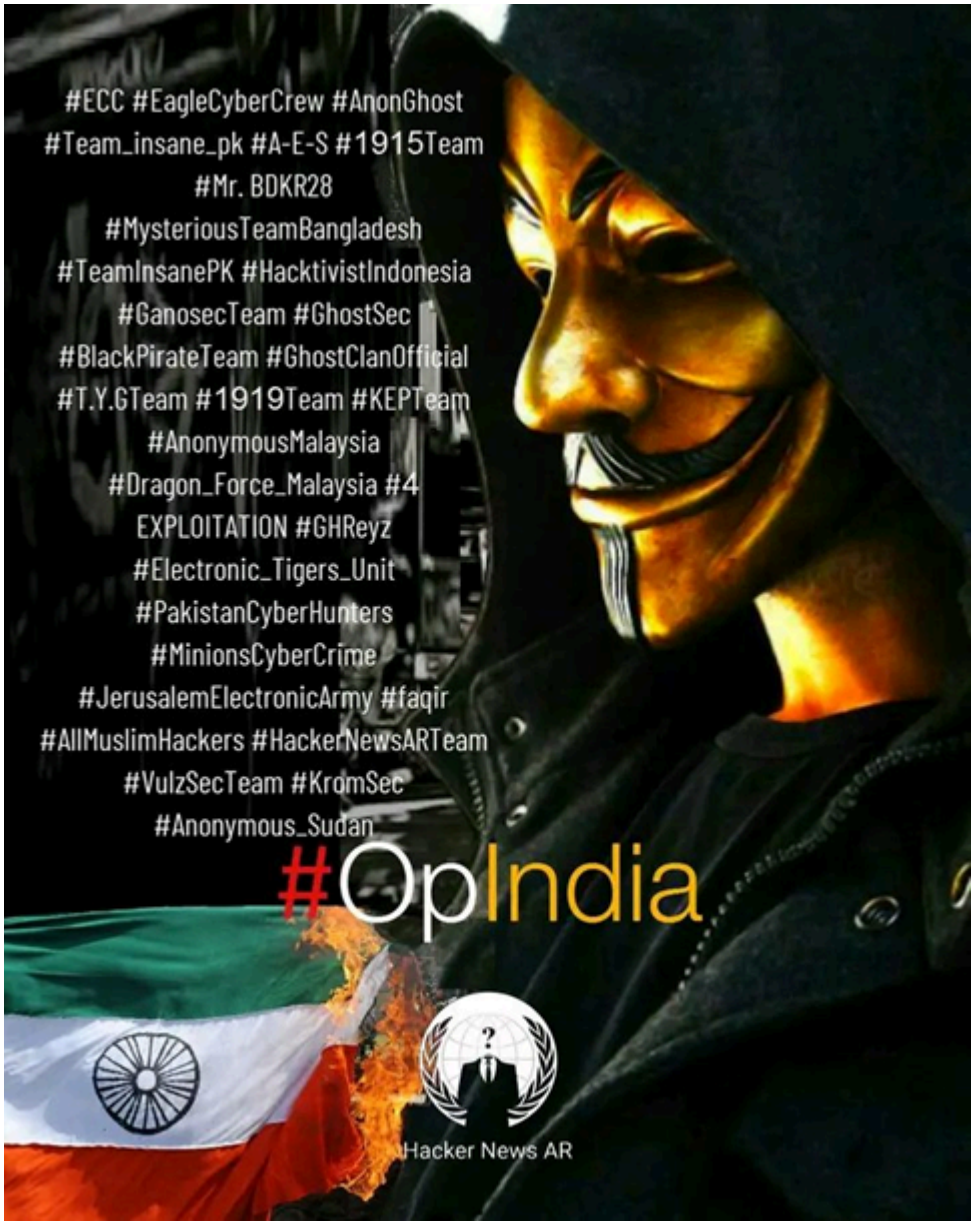


Figure 6: Announcement post of the OpIndia campaign

The following groups are involved in this campaign:

Mysterious Silent Force	Dragon Force Malaysia
Mysterious Team Bangladesh	4 EXPLOITATION Channel
Mysterious Team Bangladesh	PAKISTAN CYBER HUNTERS
EAGLE CYBER CREW	VulzSec Team
AnonGhost	Hacktivist Indonesia
Team_insane_pk official	TYG Team
A-E-S	1919 Team

1915 Team	KEP Team
GANOSEC TEAM	Anonymous Sudan

The campaign claimed to compromise the government websites of the state of Kerala, Rajasthan, Maharashtra, and Jammu & Kashmir, the Income Tax portal, the AICTE site, and allegedly leaked data related to them.

Reprisal Attacks

In retaliation to attacks on Indian infrastructure, a few Indian-sympathizing hacktivists emerged from the shadows. They publicized their claims of DDoS on organizations from Bangladesh, Indonesia, Malaysia, and Pakistan on social media and their Telegram channels.

Among many such small factions identified recently, we observed the following groups leading a coordinated wave of attacks:

Anonymous India	Mariana'S Web
Team UCC Operation	Indian Cyber Mafia
Indian Cyber Force	Team 1-4-1
Kerala Cyber Xtractors	

These groups have launched retaliatory campaigns under the monikers:

op_payback	TROLL_KANGLADESH
op_malay	OPPAYBACK_BD
op_indo_kids	OP_BD
OPPAYBACK_MY	op_porkis
OPMALAYSIA	OP_PK
OP_MY	op_pak
OPHABIBI	Payback2023
op_bd_skids	TROLL_KANGLADESH

Conclusion

Over the years, Hacktivism has become more cynical. Once a tool to voice social and political change, it has evolved into a nefarious apparatus of across-the-border crime to further their ideological agendas, disrupt government and business, and create social disharmony. Over the last year, we have also observed the emergence of state-sponsored and destructive hacktivism.

Initially started as a tool to promote religious freedom and human rights, Hacktivism has eventually transpired into online hate, discrimination, and even violence in some cases. It is important to balance the need for religious expression and activism with the need for tolerance, respect, and security in the online world. As the tactics and ideologies in hacktivism continue to evolve, individuals and governments must take steps to ensure regulated online activism and build a tolerant online community.
