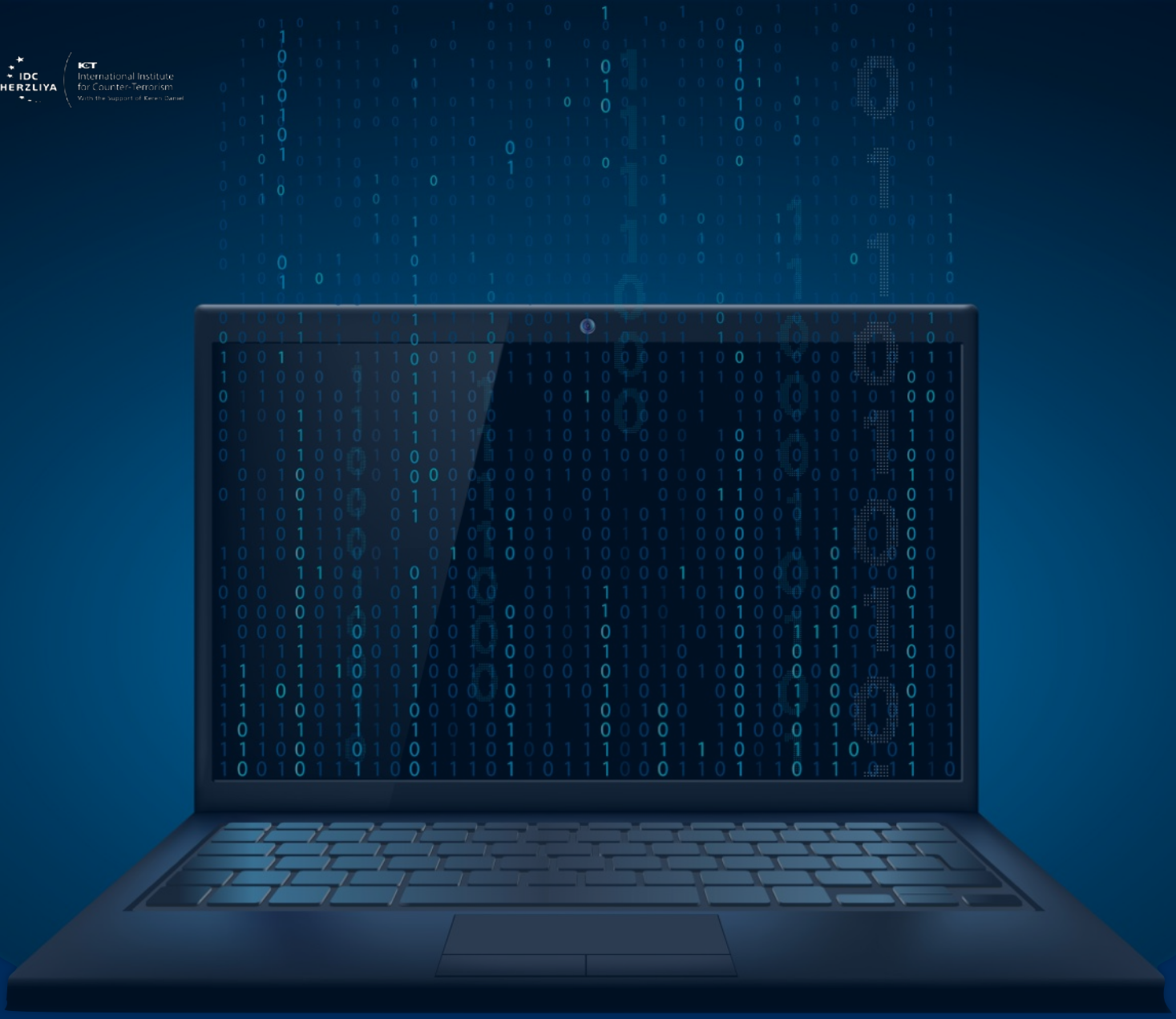
IDC HERZLIYA
ICT International Institute for Counter-Terrorism
With the support of Keren Daniel



# IS-Supporting Hacktivists in Southeast Asia

## *ABOUT THE ICT*

Founded in 1996, the International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counter-terrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense policy.

ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.

## *ABOUT ICT CYBER-DESK*

The Cyber Desk Review is a periodic report and analysis that addresses two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse) and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack).

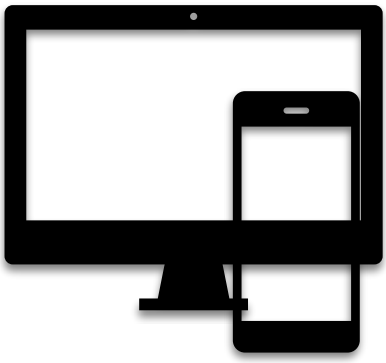
The Cyber Desk Review addresses the growing significance that cyberspace plays as a battlefield in current and future conflicts, as shown in the recent increase in cyber-attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations

# Key Findings

***There is a growing trend of hacktivism activities in Southeast Asia, including Web site defacement, distributed denial-of-service (DDoS) attacks and information leaks. One group that operates using this strategy is the United Cyber Caliphate (UCC) collective, which operates with the support of the Islamic State (IS).***

***The increase in the Islamic State's cyber activity in Southeast Asia is a result of its physical expansion into this region due to the loss of its core territory in Iraq and Syria. The region of Southeast Asia is characterized by poverty, unemployment and a Salafist worldview, which are risk factors that expose the youth of the region to radicalization.***

***The cyber environment in Southeast Asia is characterized by rapid growth, poor information security and increasing levels of cyber-attacks. Combined with growing social dependence on connection technologies and the presence of a group of hacktivists, these elements will produce a real threat in the coming years.***



# Introduction

The Islamic State (IS) is a prominent presence on the Internet. The bulk of its cyber activities are for propaganda, communication or other logistical purposes, and only a few activities involve computer technologies as a weapon or target.[1] While media groups that published and disseminate propaganda online have official status and are subject to the organization's media rules, the IS has never officially recognized an offensive hacker group.[2] This fact led to the creation of a diverse *collective* of hacker groups that operate unofficially with the organization's support and are identified with the organization by name and logo only – the United Cyber Caliphate (UCC).[3]

# Cyber-Attacks by the Islamic State

In recent years, hackers who identify themselves with IS activities have carried out actions in cyberspace that do not amount to a physical cyber threat or actual damage. These actions mainly included defacing various Web sites around the world, hacking user accounts on social media networks, and leaking personal information from databases of organizations and other entities.[4] In addition, members of the collective reported carrying out distributed denial-of-service (DDoS) attacks. The use of these cyber-attacks is characteristic of a *specific* type of hacker known as "hacktivists". Hacktivism refers to hackers who are motivated by protest over various issues, such as political, social, national or ideological motivation.[5] Most hacktivists do not openly refer to themselves as such, and the term is mainly used by researchers, journalists, and information security professionals to distinguish between different types of threats in cyberspace. The turn to hacktivism

[1] Conway, M. (2002). Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet. Dept. of Political Science, Trinity College, Dublin Ireland. *First Monday*.
[2] Tacit consent
[3] Bernard, R. (2017) These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of Islamic State, *Journal of Cyber Policy*, 2:2, 255-265.
[4] Pavel, T. (2017). Physical Threats in Online Worlds — Technology, Internet and Cyber under Terror Organization Services; a Test Case of the Islamic State", *International Journal of Information Security and Cybercrime 6.* Available online at: http://www.ijisc.com/articles/2017-01-09.pdf accessed 10.12.2018
[5] Penny Cumming (2017) Hacktivism: will it pose a threat to Southeast Asia and, if so, what are the implications for Australia? Indo-Pacific Strategic Digest, Australian Army

stems from the relative ease and low cost of such campaigns. People without technical skills can use free and user-friendly tools to carry out DDoS attacks, for example.[6]

The following are examples of cyber activities that were carried out by the UCC collective in the summer of 2018. The list is based on self-reports of the groups collected through WEBINT. It should be noted that this is a partial and incomplete list:

- The IS-supporting hacktivist group, Anshar Caliphate Army, is part of the UCC collective. The group was first documented in June 2018 in closed Telegram groups in which it declared itself one of the groups operating within the UCC collective. Language analysis revealed that the origin of this group is *Indonesian*.


*A poster of the Anshar Caliphate Army group*

- On July 27, 2018, the group published a poster detailing the cyber-attacks it claimed to have carried out between May and July 2018 in the framework of the #OpTheWorld campaign. It listed 160 Web sites that were defaced, and 110 Facebook and 20 Instagram accounts that were

[6] Dorothy Dennings (08.09.2015) The Rise of Hacktivism. Georgetown Journal of International Affairs. Available at: https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism Accessed 13.12.2018

hacked. The attacks targeted accounts and Web sites from a range of countries: India, Canada, Russia, England, United States, Israel, Holland, Germany, France, Brazil, Indonesia, Taiwan and China.


*The announcement published by the Anshar Caliphate Army*

- On July 9, 2018, the UCC collective published an announcement according to which, 21 days after the attack on *East Asian countries*, the Caliphate's hackers hacked at least 213 Web sites in Thailand, the Philippines, Indonesia and South Korea. In addition, members of the group also shut down close to 530 Web sites using DDoS attacks. According to the announcement, more than 700 accounts on social networks were hacked, most of them belonging to military personnel among Muslims who had become corrupt and Crusaders in these areas.


*The announcement published by the UCC*

- On August 28, 2018, the UCC collective published an infographic about the cyber-attacks that it carried out over a 70-day period beginning on May 19, 2018 (the third day of the month of Ramadan). The attacks included the shutdown of 770 Web sites using DDoS attacks, the breach and destruction of over 900 international sites, and the breach of over 1,500 social media accounts. The following groups participated in the attacks: Anon Terror, Team System DZ, Islamic Intelligence, Caliphate Cyber Army, Anshar Caliphate Army, Ghost Caliphate Section, Sons Caliphate Army and Fighter Muslim Cyber Caliphate. The infographic was distributed on a Telegram channel in Arabic and English, and was accompanied by text stating that *most of the attacks noted in the infographic took place in East Asia* and in the framework of the #OpTheWorld cyber campaign.


*The infographic published by the UCC*

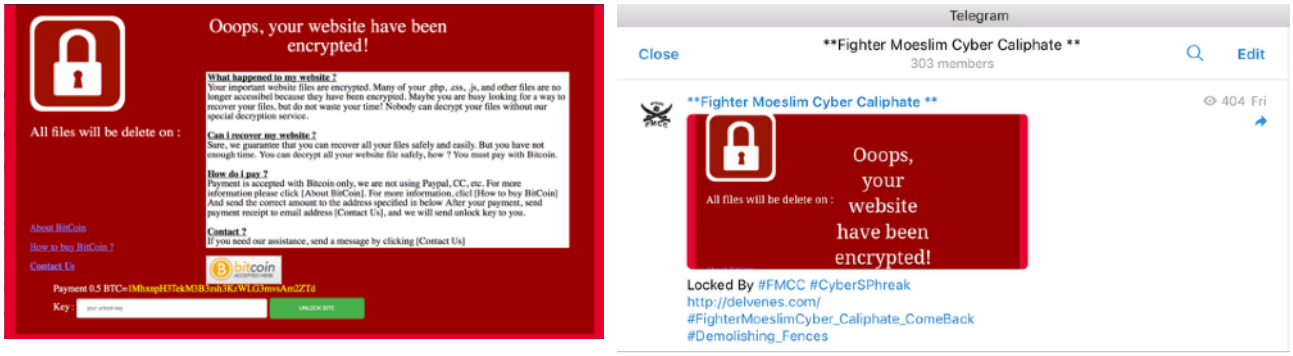
- The UCC collective has been steadily growing since the rise of the first group identified with it, the Cyber Caliphate. The group surfaced in 2014, immediately after the declared establishment of the Caliphate, and was led by Jundaid Hussain. Hussain was born in 1994 and fled from Britain to join the IS in 2013 after serving a prison term for hacking into the email account of former British Prime Minister Tony Blair. From his seat at the base of the IS in Raqqah, Syria, he recruited and cultivated the Cyber Caliphate that he foresaw until his assassination in an American drone attack in August 2015 in Raqqah;[7] Since then there has been an increase in the number of active groups, and five years later the collective is now comprised of about ten groups.[8] Moreover, the above case studies *reflect a growing increase in the scope of IS-supporting hacktivist activities in Southeast Asia*. This can be deduced from language analysis combined with their choice to attack targets in East Asian countries, alongside the infographic's emphasis that most of the attacks took place on the East Asia front.

**The above case studies reflect a growing increase in the scope of IS-supporting hacktivist activities in Southeast Asia**

[7] Alhouri, L., Kassirer, A., and Nixon, A. (2016). Hacking for ISIS: The emergent cyber threat landscape. *Flashpoint*. https://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf . Accessed 04.12.2017.
[8] As of July 9, 2018, the following groups are listed in the publication by the Fighter Moeslim Cyber Caliphate (FMCC) group: Caliphate Cyber Army, Ghost Caliphate Section, Anon Terror, Fighter Muslim Cyber Caliphate, Sons Caliphate Army, Islamic Intelligence, Anshar Caliphate Army, Al Barra Bin Malik Battalion, Team Systems DZ, Al Siddiq Battalion.

# Financing and Recruitment via the Internet

This was not the first time activity by this collective was documented in this region. On May 26, 2017, following the extensive Wannacry cyber-attack that took place during that month, a screenshot was uploaded to the Telegram channel of the Fighter Moeslim Cyber Caliphate (FMCC) documenting a cyber-attack that imitated the Wannacry ransomware. The attacked site was geographically tied to Jakarta, Indonesia. This attack was unique because the choice to use the technical means of ransomware constituted a deviation from the group's modus operandi. The group usually carries out defacement of Web sites, and uses this virtual vandalism to send ideological messages expressing support for the IS. In contrast, the ransomware attack did not focus on disseminating an ideology, but rather it was intended to generate economic profit. It should be remembered that the use of terrorism for ransoms has a potential double advantage – generating economic profit to finance terrorist activities and causing economic damage to the owners of the site, which corresponds to the Islamic State's expansion towards East Asia that took place in May 2017 (detailed discussion below).[9]




*From left to right: a screenshot from the attacked site; a screenshot from the closed Telegram channel of the FMCC group*

Another documented case illustrating the logistical use of the Internet for terrorist activities is the case of Bahrun Naim. Naim, a Syrian resident of Indonesian descent, was assassinated on June 8, 2018, by a US drone in Syria after being designated a terrorist operative by the US administration in

[9] See ICT's Cyber report no. 22, page 27: https://www.ict.org.il/Article/2110/cyber-report-no-22-june-august-2017#gsc.tab=0

March 2017.[10] This designation was based on his involvement in IS operations, including assistance and coordination of attacks in his country of origin and the financing of terrorism through bitcoin and PayPal.[11] Naim grew up in Solo, which is considered a center of Islamic radicalization in Indonesia, and received certification as an information systems engineer from Surakarta State University. He was the first Southeast Asian terrorist to use bitcoin and basic artificial intelligence to disseminate content inciting to terrorism for IS supporters on the Internet. In April 2017, Naim used a bot on his site (Wahai Muslimin) that allowed visitors an interactive and instant platform to communicate with him. In addition, he used encrypted communication channels, mainly Telegram and WhatsApp, to plan and execute attacks. In response, the Indonesian government threatened to block Telegram in July 2017, but Telegram representatives focused on blocking IS-supporting content to prevent the threat from escalating. Naim continued to act discreetly. He built a platform on social networks through which he distributed propaganda, recruited fighters and created bots to disseminate content to large audiences.[12]

Naim's case is not the only one, and is part of a *wave of designations of IS-supporting terrorist operatives of Southeast Asian origin* dating back to 2015.[13] A UN report refers to the implications of recent designations, emphasizing *the central role that intermediaries in the Southeast Asian network*

---

[10] Treasury Designates Indonesian and Malaysian ISIS Operatives and Leaders (30.03.2018). Available at: https://www.treasury.gov/press-center/press-releases/Pages/sm0037.aspx

[11] Special report regarding the use of virtual currency by jihadists, published by the ICT Cyber Desk. Available at: https://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pdf

[12] Rohan Gunaratna (03.10.2018) Death of Bahrun Naim: Mastermind of Terror in Southeast Asia. RSIS Commentary Rajaratnam School of International Studies. Available at: https://www.rsis.edu.sg/wp-content/uploads/2018/10/CO18161.pdf Accessed 13.12.2018

[13] For example, see: Two fighters from Jemmah Anshorut Tauhid (an organization influenced by the Islamic State that swore allegiance to it) of Indonesian descent were designated terrorists on September 29, 2015, at: https://www.treasury.gov/press-center/press-releases/Pages/jl0188.aspx ;Two fighters of Indonesian origin were designated terrorists due to their membership in the Islamic State, dissemination of an IS-supporting ideology in Indonesia and involvement in the Jakarta terrorist attacks. The designation was approved on January 10, 2017 at: https://www.treasury.gov/press-center/press-releases/Pages/jl0698.aspx; The Indonesian Jamaah Ansharut Daulah organization that swore allegiance to al-Baghdadi was designated a terrorist organization on January 10, 2017 at: https://www.state.gov/j/ct/rls/other/des/266772.htm; An Islamic State fighter was designated a terrorist on February 9, 2018 for providing substantial financial and technological assistance to the Islamic State network in the Philippines, at: https://home.treasury.gov/news/press-release/sm0284; The Islamic State's branch in the Philippines, with an emphasis on the Maute group, was designated a terrorist organization on February 27, 2018, at: https://www.state.gov/r/pa/prs/ps/2018/02/278883.htm; A fighter of Filipino origin was designated a terrorist on February 28, 2018 for providing substantial financial and technological assistance to the Islamic State in the Philippines; Three Islamic State fighters of Malaysian, Indonesian and Filipino origin who participated in a beheading video were designated terrorists on August 24, 2018 at: https://home.treasury.gov/news/press-releases/sm469 ;All accessed on December 13, 2018

*play in finance, weapons and training*. It further emphasized the ties between international players, local operatives and the IS core. For example, intermediaries enabled money transfers from the IS core to IS branches in the Philippines, and organized bomb assembly and weapons training for new recruits by the Indonesian Jamaah Ansharut Daulah (JAD) organization, which is identified with the IS, in camps in the Philippines.[14]

## The Invasion of Southeast Asia

The growing trend of IS cyber activities in the Southeast Asia region is not taking place in a vacuum, and is the result of the Islamic State's physical expansion to this region. For instance, two terrorist attacks took place in Southeast Asia in May 2017. The first took place in Jakarta, Indonesia, in which two suicide terrorists detonated next to a bus station. Three police officers were killed in the attack and 12 civilians were injured. The IS claimed responsibility for the attack. The second attack was the takeover of the city of Marawi, which is located on the island of Mindanao in the Philippines. The attack claimed the lives of at least 27 Filipino civilians and 15 soldiers.[15] In addition, over the course of two days in May 2018, Indonesia suffered a wave of attacks, with JAD cells and their families carrying out two terrorist attacks that killed dozens of people. The third attack was thwarted by the authorities.

It should be noted that Abu Sayyaf, a jihadist group affiliated with the IS, has been operating in the Philippines since the early 1990's. Abu Sayyaf was designated a terrorist group by the US in 1997 and is considered the most violent group operating in the Philippines, whose activities include kidnappings for ransom, the use of explosives, beheadings, murder and extortion.

South and Southeast Asia have the largest Muslim population in the world. However, this is not the only reason for the Islamic State's desire to expand into the region on the one hand, and for the

[14] UN Security Council S/2018/705 (July 16, 2018) report https://undocs.org/S/2018/705 accessed December 13, 2018, page 18, paragraph 70
[15] Ibid.

locals' identification with the IS on the other hand. In Southeast Asia, there is a high unemployment rate among young men, and conservative Salafist groups invested enormous resources in this infrastructure in the region. For example, hundreds of schools and charities have been established in Indonesia, Malaysia and Bangladesh, including the Saudi organization, Dewan Dakwah Islamiyah Indonesia, which promotes a Salafist agenda in Indonesia.[16] The religious fanaticism of the Islamic State is in line with the prevailing attitude in the region. Religious Muslims from the Southeast Asian region feel a connection to the IS and identify with its values.[17]

This perception is growing with the work of the radical cleric, Aman Abdurrahman (aka Oman Rochman).[18] Abdurrahman is the leader of the designated terrorist organization, JAD (see above), and is considered the de-facto leader of all IS supporters in Indonesia.[19] The cases of incitement to terrorism attributed to Abdurrahman include the shooting and suicide attack in Jakarta in 2016 that claimed the lives of four civilians; this was the first attack in Southeast Asia for which the IS claimed responsibility.[20] On June 22, 2018, Abdurrahman was sentenced to death;[21] although he is currently serving a prison sentence for incitement to terrorism, Abdurrahman disseminates his ideology via the Internet and translates IS propaganda to Indonesian.[22]

Indeed, along with the spread of propaganda on the Internet and on social networks encouraging the execution of "lone wolf" attacks in the West, the IS publishes a propaganda campaign promoting radicalization in the Southeast Asia region.[23] Near the date of the attacks mentioned above, evidence of a clear trend of concentration on this geographical area was found in the jihadist

---

[16] Fred R. Von Der Mehden (2014) Saudi religious influence in Indonesia. Middle East institute/ Available at: https://www.mei.edu/publications/saudi-religious-influence-indonesia Accessed 10.12.2018

[17] Joseph Chinyong Liow. ISIS Goes to Asia, Brookings, 21.09.2014. https://www.brookings.edu/opinions/isis-goes-to-asia/ Accessed 10.12.2018

[18] Ibid.

[19] Jamaah Ansharut Daula (JAD) was designated a terrorist organization by the US State Department on January 10, 2017. https://www.state.gov/j/ct/rls/other/des/266772.htm Accessed December 10, 2018

[20] https://www.straitstimes.com/asia/se-asia/indonesian-cleric-aman-abdurrahman-sentenced-to-death-for-inciting-terror-attacks Accessed 10.12.2018

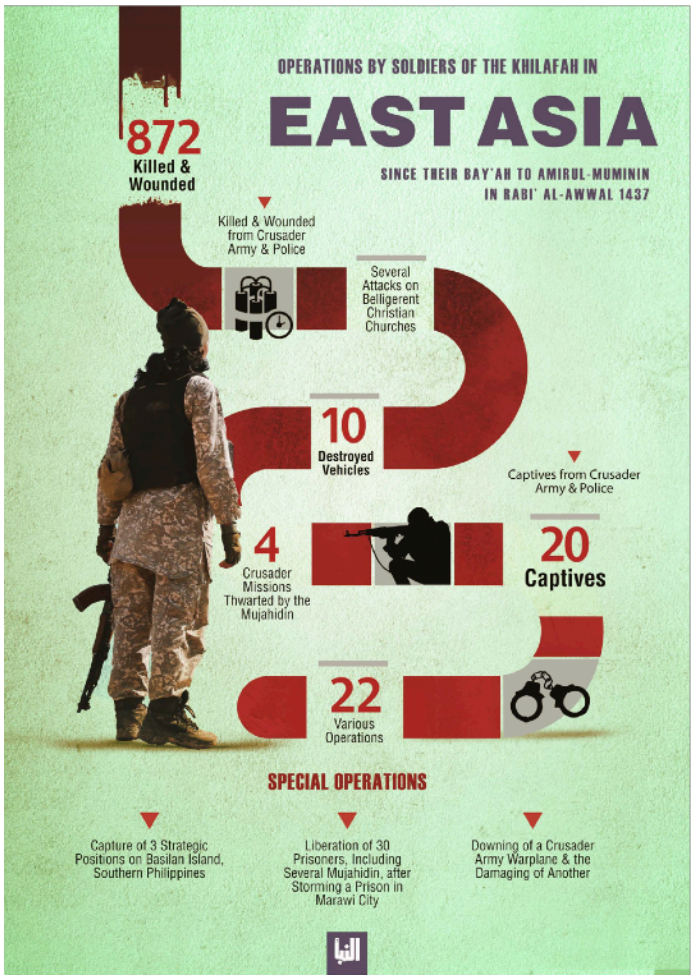
[21] https://www.nytimes.com/2018/06/22/world/asia/indonesia-isis-aman-abdurrahman.html Accessed 10.12.2018

[22] Joseph Chinyong Liow. ISIS Goes to Asia, Brookings, 21.09.2014. https://www.brookings.edu/opinions/isis-goes-to-asia/ Accessed 10.12.2018

[23] https://www.carnegiecouncil.org/publications/ethics_online/0122 Accessed December 10, 2018

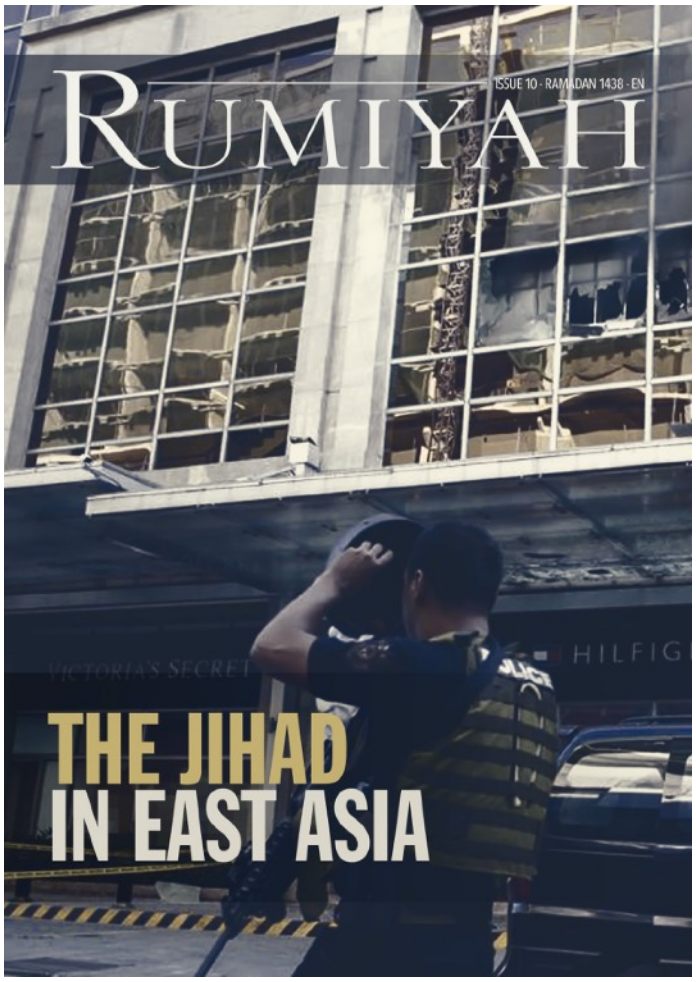
discourse on Telegram among groups of the organization's supporters. The following are some examples of this propaganda:

- In April 2017, an infographic was distributed on Telegram that was taken from the eighth issue of the magazine, *Rumiyah*, and presented data about the operations carried out by soldiers of the Caliphate in East Asia. The infographic counted 872 killed and wounded among the Crusader security forces; several attacks against the enemy's Christian churches; 10 Russian vehicles destroyed; 20 security forces taken captive; and four Crusader attacks thwarted by the mujahideen. It also counted three special operations, including the strategic capture of three officials on the island of Silan in the southern Philippines; the release of 30 prisoners, including mujahideen, in an assault on a prison in the city of Marawi; the downing of a war plane belonging to a Crusader army and damage to another plane.




*Rumiyah, issue 8*

- In light of the attacks described above, the title page of the tenth issue of *Rumiyah*, which was published in June, was dedicated to East Asia. On page five, it stated that the attack in Manchester was consistent with what many analysts have claimed for some time: that, with the loss of territory in Iraq and Syria, the IS would shift its focus to carrying out attacks on Crusader lands. What many analysts failed to admit, it stated, is that losing territory is nothing new for the IS. The loss of territory only pushes the IS to re-organize, redouble its efforts, and rekindle the flames of war. This is why, it was claimed, it was no surprise when far from Manchester, the soldiers of the Caliphate in East Asia stormed the city of Marawi on the island of Mindanao in the southern Philippines, where they raised the flag of the IS.




*Rumiyah, issue 10*

- In August 2017, Al-Hayat jihadist media institution published the third video in the series, "Inside the Khilafah". The video showed several IS fighters from Marawi and appealed to the East Asian people, mainly in Indonesia, Malaysia, Brunei, Thailand and Singapore, to come to Dar al-Islam in Marawi.


*A screenshot from Inside the Khilafah no. 3*

- In September 2017, Al-Hayat jihadist media institution published the fourth video in the series, "Inside the Khilafah". In the video, Abu Uqayl, of Singaporean origin, addressed the mujahideen in East Asia to thank them for expanding the structure of the Caliphate, thereby bringing happiness to the hearts of believers and anger to the hearts of Allah's enemies. He called on them to continue along this path in order to win Allah's love and join the ranks of the mujahideen in East Asia to strike the Crusaders.


*A screenshot from Inside the Khilafah no. 4*

# The Cyber Environment in Southeast Asia

In Southeast Asia there is a growing trend of hacking activities. While the media attributes these activities to groups of hackers supported and directed by China or Russia, many of these activities appear to be carried out by hacktivist entities.[24] In the past, hacktivists carried out defacement and DDoS attacks in response to the maritime conflict in the South China Sea. In the standstill between Vietnam and China in 2011, between the Philippines and China in 2012; between Taiwan and the Philippines in 2013; between Vietnam and China in 2014; between Vietnam, the Philippines and China in 2015.[25] A more recent example is from March 2018 when the Indonesian police arrested 14 people suspected of membership in a radical cyber network called the Muslim Cyber Army. The suspects were accused of using hacking, influence campaigns and expressions of hatred on the Internet to bring about a change in the nature of Indonesian culture toward conservatism.[26]

**The legislative and regulatory systems in the field of information systems protection and the implementation of information security practices in this region are not sufficiently developed and are purely voluntary;**

**more than anything, there is a lack of strategic thinking about information security.**

These attacks are made possible due to the characteristics of the local cyber environment. The Southeast Asian cyber environment is in the midst of rapid processes of increased use, and the region's population is the fourth largest in terms of Internet and smartphone use. However, *both the*

[24] Penny Cumming (2017) Hacktivism: will it pose a threat to Southeast Asia and, if so, what are the implications for Australia? Indo-Pacific Strategic Digest, Australian Army

[25] Marie Baenzer (August 2018) Hotspot analysis: Use of cyber tools in regional tensions in Southeast Asia. Center for Security Studies, Zurich. Available at:http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-05.pdf Accessed 12.12.2018

[26] Vincent Bevuns (01.03.2018) Indonesian police arrests 14 suspected members of radical Islamic cyber network. Available at: https://www.washingtonpost.com/world/asia_pacific/indonesia-police-break-up-islamist-cyber-network-promoting-extremism/2018/03/01/ff575b00-1cd8-11e8-98f5-ceecfa8741b6_story.html?utm_term=.42cf1db4113d. Accessed 12.12.20189

*legislative and regulatory systems in the field of information systems protection and the implementation of information security practices in this region are not sufficiently developed* and are purely voluntary;[27] more than anything, *there is a lack of strategic thinking about information security*.[28] The rapid increase in the use of information technologies, combined with a lack of adequate information security, is fertile ground for the prominent trend of dangerous cyber activities in the region.[29] For example, Indonesia is the sixth largest country in terms of Internet users (over 80 million) and still fell victim to 3.9 million cyber-attacks between 2010 and 2013, including a period of 10 months in which most of the attacks were against government sites.[30] Attacks against government sites also characterize the UCC collective. For example:

- On May 27, 2017, CybersSPhreak, the leader of the FMCC group, carried out a defacement attack against an Indonesian tourism site. On the site's homepage, a message was left to Jokowi DogDog, a mockery of the name of the head of state, Joko Widodo, who was also called a heretic. The caption protested Widodo's defense of non-Muslims and failure to protect his own people.


*A screenshot of the defacement attack carried out by the leader of the FMCC against an Indonesian Web site*

[27] Lee Mihyun, 'Southeast Asia begins to prepare for cyber war: India turns to AI', *Huffington Post*, 23 January 2017, available athttps://www.huffingtonpost.com/asiatoday/southeast-asia-begins-to_b_14334812.html accessed 11.12.2018
[28] ATKearny (2018) Cybersecurity in ASEAN - An urgent call to action. Available at: https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-in-asean/files/assets/common/downloads/publication.pdf Accessed 11.12.2018
[29] Penny Cumming (2017) Hacktivism: will it pose a threat to Southeast Asia and, if so, what are the implications for Australia? Indo-Pacific Strategic Digest, Australian Army
[30] Jacqueline Kelleher, 'Indonesia launches Cyber Security Agency', *OpenGovAsia*, 15 September 2015, available at <http://www.opengovasia.com/ articles/6563-indonesia-launches-cyber-security-agency-in-wake-of-growing-threat- landscape> accessed 11.12.2018

- On August 13, 2018, the Anshar Caliphate Army group published a video in which it appealed to IS supporters in Indonesia to join the cyber campaign, and carry out attacks against the Indonesian government and social media accounts. The video included English audio and subtitles in Indonesian. The campaign was scheduled for August 17 and called #OpTheWorld. The campaign appeared to be a response to the Indonesian government's decision to block IS-supporting[31] content by implementing a "crawling" system to identify and alert against pornographic/radical content.[32] It is possible that it was also a response in protest of Abdurrahman's sentence.


*A screenshot from the video by Anshar Caliphate Army*

[31] Amy Chew (23.08.2018) Pro-Islamic State hackers threaten terror attacks against Indonesian government. Available at: https://www.channelnewsasia.com/news/asia/pro-islamic-state-hackers-threaten-terror-attacks-against-10644690 Accessed 12.12.2018

[32] Available at: Ed Davies, Cindy Silviana (19.02.2018) New Indonesia web system blocks more than 70,000 'negative' sites. https://www.reuters.com/article/us-indonesia-communications/new-indonesia-web-system-blocks-more-than-70000-negative-sites-idUSKCN1G30KA Accesses 12.12.2018

# Discussion and Conclusions

In Southeast Asia, there is a growing trend of hacktivism activities, including Web site defacement, distributed denial-of-service (DDoS) attacks and information leaks. The United Cyber Caliphate (UCC) collective, which operates with the support of the Islamic State (IS), employs this strategy. The prevailing view is that due to the low offensive level of these activities, they are a transitional stage on the way to acquiring higher level offensive capabilities. Although this is a solid and valid option, in our assessment, the UCC collective will continue to act within the framework of hacktivist attacks; it will not want to raise the technical level of the attacks but will continue to increase the number of participants and the scope of activity. The UCC does not have the realistic ability to deal with the cyber defense systems of state players and, therefore, its strategic consideration is to carry out simple attacks that will attract maximum attention. An analogy can be made to attacks in the physical world; similar to the situation today in which terrorist organizations have no realistic possibility of carrying out mega-attacks like the attacks on the Twin Towers or sending suicide bombers to city centers and so they turn to simple acts, such as stabbings.

The increase in the Islamic State's cyber activity in Southeast Asia is a result of its physical expansion into this region. The loss of its core territory in Iraq and Syria led to the Islamic State's incursion into other areas, including Southeast Asia, which are characterized by poverty, unemployment and a Salafist worldview, which are risk factors that expose the youth of the region to radicalization. The organization is transforming itself from a state structure into a decentralized network of covert cells.[33] It is necessary to pay attention to the wave of designations of IS operatives of Southeast Asian origin and their central role in IS cells in Southeast Asia in terms of financing, weapons and training.

[33] Azani Eitan (May2018) Global Jihad — The Shift from Hierarchal Terrorist Organizations to Decentralized Systems. Available at: https://www.ict.org.il/images/Global%20Jihad%20–%20The%20Shift%20from%20Hierarchal.pdf. Accessed 13.12.2018

The cyber environment of the region is a hotbed for cyber-attacks and the region's increasing strategic importance makes it a prime target for cyber-attacks. Countries in the region have different degrees of cyber readiness; the absence of a unified framework makes the region's information security voluntary, which in turn leads to a lack of risk assessment and low resilience. The region's developing information security industry faces a lack of cyber capabilities and expertise, along with partial products and few comprehensive solutions.[34] Most of all, *there is an absence of strategic thinking patterns, policy preparedness, and institutional oversight regarding information security*. These gaps expose Southeast Asia to cyber-attacks in general, and to attacks by hacktivists operating with IS support in particular, and we believe that hacktivism in support of the IS in Southeast Asia is likely to expand in the coming years.

[34] ATKearny (2018) Cybersecurity in ASEAN - An urgent call to action. Available at: https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-in-asean/files/assets/common/downloads/publication.pdf Accessed 11.12.2018

## CYBER-DESK TEAM

Dr. Eitan Azani, Deputy Executive Director, ICT

Nadine Liv, Researcher, ICT

Dr. Michael Barak, Team Research Manager, ICT

Adv. Uri Ben Yaakov, Senior Researcher, ICT

## CYBER-DESK CONTRIBUTORS

Oren Elimelech, cyber security expert, researcher & consultant

Ms. Sigalit Maor-Hirsh, terrorism and communication expert

Adv. Deborah Housen-Couriel, cyber security and international law expert

Mr. Shuki Peleg, head of Information security and cyber at MATAF, Israel

Dr. Harel Menashri, research fellow, ICT, & cyber, information security & technological intelligence expert, Israel