

An abstract pattern of glowing blue lines and nodes, resembling a circuit board or a network map, set against a dark blue background.

لا إله إلا الله



**SPECIAL REPORT:**  
**KILL LISTS FROM PRO-IS HACKING GROUPS**

---

## **CONTENTS**

I. Introduction,	2
II. Executive Summary,	3
III. Identifying Groups,	4
A. Caliphate Cyber Army,	5
B. United Cyber Caliphate,	6
C. Islamic State Hacking Division,	7
IV. Kill Lists and Analysis,	8
A. CCA Releases Purported Employee Information of 56 NJ Transit Police Staff,	9
B. CCA Disseminates Personal Info of U.S. Police in Minnesota as "Wanted to be Killed",	10
C. UCC Claims Hack of Tennessee County Database,	11
D. UCC Posts Names and Addresses of 3,600 Purported NY Citizens,	12
E. UCC Claims Hacking U.S. State Department,	13
F. ISHD Distributes List of Names, Addresses of 76 Alleged U.S. Military Drone Personnel,	14
G. UCC Releases Second Part of Data from Alleged U.S. State Department Hack,	15
H. UCC Posts Names, Addresses of 1,500 Purported Texas Residents,	16
V. Conclusion,	17



## I. INTRODUCTION

Recently released “kill lists” associated with the Islamic State (IS, also known as ISIS) have highlighted an evolving and increasingly implemented terror tactic. These lists, with targets spanning drone operators to random civilians, appear to have achieved at least part of their presumed intentions: heightened alert by government workers, FBI visits to startled civilians, and significant media attention.

Kill lists have long been released officially by jihadi groups, but it wasn’t until recently that self-proclaimed hacking groups began releasing their own kill lists. Last year, a pro-IS hacking group by the name “Islamic State Hacking Division” (ISHD) released a list of 100 military personnel in March of 2015, marking the first such list produced by a jihadi hacking entity. The group followed up with another list of 100 U.S. military personnel on September 11 of that year.

In just over a year, kill lists from pro-IS hacking groups have not only become more abundant, but have also expanded in terms of target selection. Previous kill lists by pro-IS hacking groups, such as those by the aforementioned ISHD, showed conventional focuses on government and military personnel perceived to be taking part in the fight against IS. However, between March and May of this year, kill lists by these groups have expanded beyond conventional criteria to random civilian targets, instructing to “shoot them down.”

Though media headlines have frequently used phrases along the lines of *ISIS Kill Lists*, these releases’ sources and content are more diverse than such titles imply. The lists have come from numerous pro-IS “hacking” groups, which vary in technical abilities, target selections, methods of disseminating the lists, and extent of connection to IS.

***IN JUST OVER A YEAR, KILL LISTS FROM PRO-IS HACKING GROUPS HAVE NOT ONLY BECOME MORE ABUNDANT, BUT HAVE ALSO EXPANDED IN TERMS OF TARGET SELECTION.***

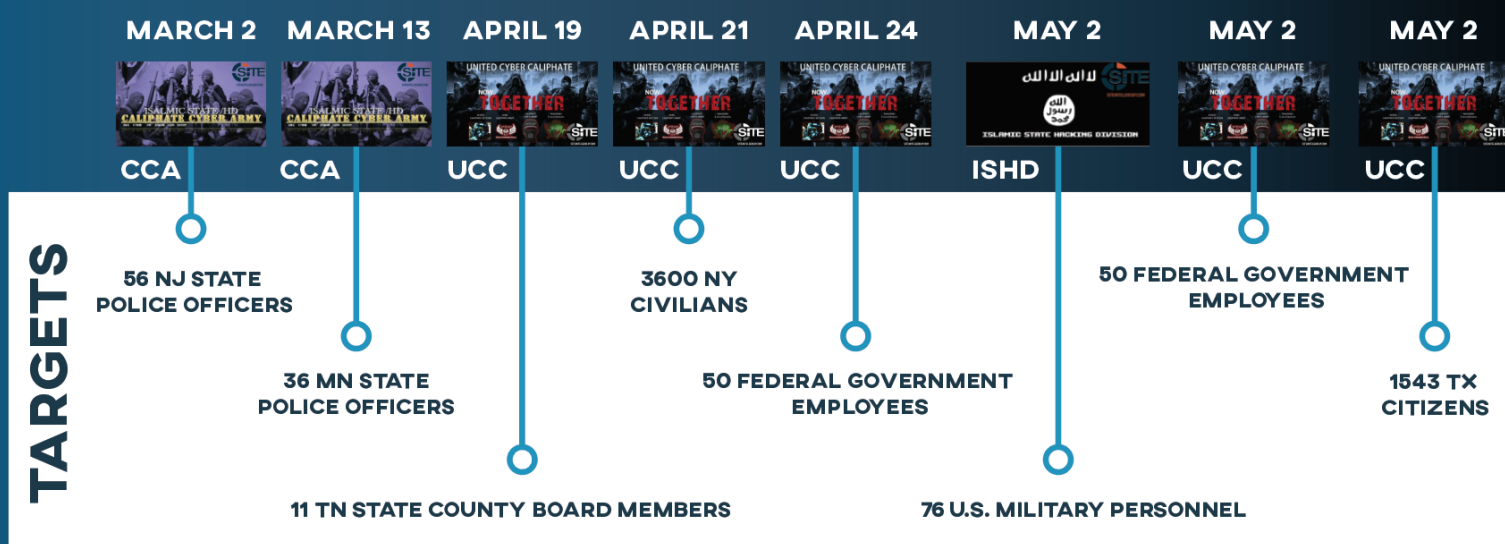
In wake of these developing trends, SITE’s Dark Web and Cyber Security service has prepared the following report to provide a chronology and analysis of kill lists released by pro-IS hacking groups since March 2 of 2016. The report will also describe past kill lists and activity by pro-IS hacking groups to provide necessary context to these recent releases.

## II. EXECUTIVE SUMMARY

Between March 2 and May 2 of 2016, SITE documented and analyzed eight kill lists released on social media by pro-IS hacking groups. The lists were released by three pro-IS hacking groups: the Caliphate Cyber Army (CCA), the Islamic State Hacking Division (ISHD), and the United Cyber Caliphate (UCC). Analysis of these kill lists indicate three kinds of targets, all of which pertaining to Americans: Federal government and military personnel; state and local government workers; and random civilians.

A chronological overview of these groups' kill lists released in this time period (explained in further detail in the Kill Lists and Analysis section of this report) follows:

## TIMELINE



None of the eight kill lists—with the exception of those by the ISHD—were promoted or disseminated by official IS channels. The lists were, however, heavily promoted by IS fighters and supporters on social media. Furthermore, though the kill list of New York residents was taken down by its hosting site within 48 hours, those pertaining to Tennessee and Texas residents are still available at the time of writing this report.

Lists released by the CCA marked the first to deviate from traditional targets toward random civilian ones, differing from those released by the ISHD. This embrace of random targets, though new within the context of hackers' kill lists, is nonetheless consistent with IS' methodology, and demonstrates application of attack instructions from IS' leadership and affiliates.

While some information about the listed individuals can be found in public records, the lists appear to be compiled via non-public sources, especially when factoring what would be immense labor and difficulty required to manually compile the information via those public

sources. This possibility is given plausibility when considering pro-IS hacking groups' previously claimed attacks, which include the CCA's (then the Cyber Caliphate) taking over a French TV station broadcast and the ISHD's release of the aforementioned kill list of nearly 1,500 U.S. military personnel. Thus, the possibility that these groups obtained hacked data for their kill lists cannot be discounted (however, neither can it be confirmed).

Further complicating such considerations are the potential means by which recent kill lists' data would have been hacked. For instance, the 1,500 U.S. military personnel's information was provided by a Kosovar hacker named Ardit Ferizi, suggesting that pro-IS hackers may at times rely more social connections than their technical abilities.

These groups have redistributed selected lists on multiple occasions, and have further promised to release additional installations of them. On May 14, for example, the UCC redistributed its May 2 list of Texans, stating, "We want them dead." Three days later, on March 17, the group threatened to release "Part 3" of its State Department kill list (detailed later in this report), stating, "We will kill you all." No such addition was released during the making of this report.

The following section provides profiles and relevant background information regarding the three identified pro-IS hacking entities.

### **III. IDENTIFYING GROUPS**

The kill lists analyzed in this report were released by three pro-IS hacking entities: the "Caliphate Cyber Army" (CCA), the "Islamic State Hacking Division" (ISHD), and an umbrella group by the name "United Cyber Caliphate" (UCC). These groups exist within a larger community of hacking groups, which similarly perform cyber-attacks in support of IS and garner support from IS' followers.

The connections between each of these three groups are in some ways unclear. While the CCA often participates in activity attributed to the UCC umbrella group to which it belongs, the ISHD has not collaborated with these groups in a publicized or formal fashion. However, this does not discount the possibility that the groups communicate and/or coordinate privately, as many IS-affiliated organizations tend to do. These groups also indicate varying levels of connection to IS at the organization level. The ISHD was headed by prominent IS fighter and recruiter [Junaid Hussain](#) ("Abu Hussain al-Britani"), and its kill lists were disseminated by social media accounts belonging to IS officials. Contrastingly, members of the CCA and UCC are unknown outside of their hacking aliases, and their kill lists and other releases have not been promoted by any official IS channel.

The following sections profile the aforementioned hacking entities to provide a more rounded view of their histories, affiliations, and technical abilities.





### III. A. CALIPHATE CYBER ARMY

The Caliphate Cyber Army (CCA), previously known as the “Islamic Cyber Army” or “Cyber Caliphate,” has attempted hacking operations against U.S. websites at least as early as December 2014. Today, it is one of the most consistently active groups of pro-IS hackers. The sophistication of the group’s hacking capabilities has generally remained relatively low, mostly consisting of website defacements on small businesses and organizations, while also disseminating other hackers’ kill lists (see Islamic State Hacking Division profile later in this section of the report).

The March 2016 releases of original U.S. police kill lists marked a shift in the type of attacks from the CCA. This is especially true of the list pertaining to Minnesota police, which, unlike its other releases, provided personal information not previously released or publicly available.

Kill list targets have spanned:

- NJ Transit Police
- Minnesota Police

Between March 2 and May 3 of 2016, the group has independently released two kill lists. Following the release of these lists, the CCA would become one of the primary groups within an umbrella hacking collective, profiled below.



*Example website defacement by CCA*



### III. B. UNITED CYBER CALIPHATE

The United Cyber Caliphate (UCC) is an umbrella hacking group announced on April 4, 2016 as being comprised of the CCA and at least three other pro-IS hacking groups:

- "Kalachnikov E-security Team," a close affiliates of CCA which first appeared in March 2016. The group typically performs website defacements in conjunction with CCA and provides technical guidance to IS supporters.
- "Sons Caliphate Army," which focuses on hacking Facebook and Twitter accounts.
- "Ghost Caliphate Section," a supposed cooperative effort with the "AnonGhost" hacking group (this collaboration has been disputed).

UCC releases are shared not only on its own social media channels, but also on those of member groups (including the CCA). In addition to releasing kill lists, the group has continued a similar style of cyber operations as the CCA, primarily performing website defacements.

Kill list targets have spanned:

- New York residents
- U.S. State Department personnel
- Texas residents

Between March 2 and May 3 of 2016, the group has released five kill lists.



لا اله الا الله



ISLAMIC STATE HACKING DIVISION

### III. C. ISLAMIC STATE HACKING DIVISION

Separate from the aforementioned entities is the "Islamic State Hacking Division" (ISHD), an IS-affiliated hacking group formerly run by killed IS fighter Junaid Hussain ("Abu Hussain al-Britani"). The ISHD has indicated the highest connection to IS among the three profiled groups, and is seen as the most prominent.

The group emerged in March 20, 2015 with a kill list of 100 U.S. military personnel's addresses. This was the first kill list released by a pro-IS hacking group. Following this release, the ISHD released alleged information on 10 Italian Army officers, and later, 1,500 military and government personnel.

The latter of those lists was, at the time, considered to be one of the most significant cyber-attacks committed by any pro-IS hacking group, potentially demonstrating an unprecedented, higher

level of capability. It was later discovered, however, that the list had been obtained through an associate of Junaid Hussain's, a Kosovar hacker named Ardit Ferizi (AKA "Th3Dir3ctorY"). According to the U.S. Justice Department, Ferizi had successfully hacked into servers of a U.S.-based company that held information about the personnel, which he then provided to Hussain to post online. Ferizi was subsequently charged with computer hacking, identity theft, and providing material support to IS in October 2015.

An additional list of 100 U.S. military personnel, released on September 11, 2015 (less than a month after Hussain was announced dead), would be followed by an eight-month period of inactivity by the group until its May 2, 2016 release of 76 alleged U.S. military drone personnel's names and addresses.

Kill list targets have spanned:

- U.S. Air Force, Army, and Navy
- U.S. military drone personnel
- Other U.S. military and government personnel
- Italian Army Officers



*Junaid Hussain ("Abu Hussain al-Britani")*

Between March 2 and May 3 of 2016, the group has released only one kill list.













## IV. KILL LISTS AND ANALYSIS

The inclusion of random citizens as targets in the following lists began with the UCC's April 21 release of 3,600 NY citizens. Kill lists released prior to this one focused largely on government or military targets, and did not include civilian targets. Since the April 21 release, however, two more have been released by the UCC.

Of note is that the lists of U.S. civilians have only been released by the UCC; the ISHD has only released lists of government or military-related targets.

As shown in the remainder of this section, kill lists were compiled and released in different fashions. The only list exclusively released on Twitter was the ISHD's May 2 list of U.S. drone personnel. Formats of the kill lists ranged from a spreadsheet, images styled to resemble confidential files, and plain text (downloadable or uploaded to pasting websites).

Following are summaries and analyses of the eight kill lists released by pro-IS hacking groups between March 2 and May 2 of 2016.

Hacker Group	Release Date	Type of Target	Platform	Medium of Distribution	Information Provided
Caliphate Cyber Army	3/2/2016	State police officers	 	A spreadsheet	Employee names, employee numbers, rank, gender, phone numbers, and "ship to" addresses, which include work and personal data, and "Date/Time of order."
Caliphate Cyber Army	3/13/2016	State police officers	 	Images containing text	Alleged names, addresses, email accounts, phone numbers, and insurance information
United Cyber Caliphate	4/19/2016	State county board members		Link to plain-text file hosted on file-sharing site (still available)	Full names, addresses, phone numbers, and email addresses
United Cyber Caliphate	4/21/2016	U.S. civilians		Link to a document on pasting site (removed within 48 hours)	Full names, email addresses, street addresses, phone numbers, and neighborhoods of residency
United Cyber Caliphate	4/24/2016	Federal government employees		Images containing text	Names, places of work, and phone numbers
Islamic State Hacking Division	5/2/2016	U.S. military personnel		Link to a PDF uploaded to a file-sharing website	Rank, full name, personal address, and a short description
United Cyber Caliphate	5/2/2016	Federal government employees		Images containing text	Names, places of work, and phone numbers
United Cyber Caliphate	5/2/2016	U.S. citizens		Document uploaded to a pasting site (still available)	Full names, email addresses, personal addresses, phone numbers, and IP addresses

#### IV. A. CCA RELEASES PURPORTED EMPLOYEE INFORMATION OF 56 NJ TRANSIT POLICE STAFF

**Release Date:** March 2, 2016

**Type of Target:** State police officers

**Platform of Distribution:** Telegram, Twitter

**Medium of Distribution:** Spreadsheet

**Information Provided:** Employee names, employee numbers, rank, gender, phone numbers, and "ship to" addresses, which include work and personal data, and "Date/Time of order."



Unlike prior "hacks" by the group until this point, the information in the CCA's March 2 [release](#) appeared to be neither previously-released by other hacking groups nor publicly-available. While some of the names of officers were listed on the website for the NJ Transit Police, other information, such as employee numbers, was not.

For instance, one officer (selected information redacted) is publicly listed on the official website (as appears below) of the NJ Transit Police. However, only his name, rank, email address, and phone number are provided.

Employee Information			
Rank:	Captain	Employee Name:	[REDACTED]
Phone Number:	[REDACTED]	Gender:	Male
Working Location:	[REDACTED]	Employee Number:	[REDACTED]
Date/Time of Order:	2/21/2016 6:10:37 PM	Ship To:	Work
		Address:	NJTransit Police Department 703 Ferry Street Newark, NJ 07105

It is notable that the phone number listed in the CCA's spreadsheet does not match the official one.

The names and information were redistributed on March 20 via Twitter in the form of individual images dedicated to each officer. The group also tweeted messages in Arabic directed at lone wolves purportedly in New Jersey to "kill [the personnel] wherever you find them" and to "lie in wait as a lone lion and kill them and horrify them." Other messages in English simply stated, "Wanted to be killed," as appears below:



**CALIPHATE CYBER ARMY** @PNR\_Status · 52m

#CoalitionProgress

#جيش الخلافة الإلكترونية

#CaliphateCyberArmy

مطلوب للقتل

Wanted to be killed

3

## IV. B. CCA DISSEMINATES PERSONAL INFO OF U.S. POLICE IN MINNESOTA AS "WANTED TO BE KILLED"

**Release Date:** March 13, 2016

**Type of Target:** State police officers

**Platform of Distribution:** Telegram, Twitter

**Medium of Distribution:** Images containing text

**Information Provided:** Alleged names, addresses, email accounts, phone numbers, and insurance information



The CCA [posted](#) the alleged personal information of 36 Minnesota police officers on Twitter and Telegram accounts with the message "wanted to be killed."

Additionally, this set of information came nearly two weeks after the CCA released a video showing the group's apparent access to a server of the website for the Minnesota Police and Peace Officers Association, and subsequently defacing the site. Linking that event with this release provides a strong possibility that the group obtained the information directly from the website servers, though this was never confirmed by the CCA.



Each officer had a dedicated image with their information listed. Similar to the release of NJ Transit Police, the personal information appeared to be neither previously released by other hacking groups nor publicly available.

#### IV. C. UCC CLAIMS HACK OF TENNESSEE COUNTY DATABASE

**Release Date:** April 19, 2016

**Type of Target:** State county board members

**Platform of Distribution:** Telegram

**Medium of Distribution:** Link to plain-text file hosted on file-sharing site (still available)

**Information Provided:** Full names, addresses, phone numbers, and email addresses

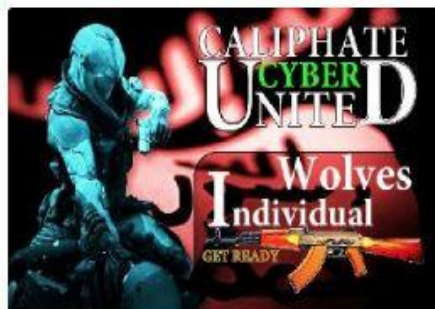


The UCC claimed [hacking a database](#) from Loudon County, TN, U.S., and disseminated 11 sets of names and personal information for lone wolf attacks.

Nine of the sets of the names and personal information were found in publicly-accessible directories of Loudon County Board Members and the City of Loudon Regional Planning Commission. The other two sets of information were found via other publicly-accessible general directories.



CALIPHATE CYBER ARMY 4/19/16



IN THE NAME OF "ALLAH"

\*\*\*\*\*

#UCC / CALIPHATE HACKERS DIVISION  
DATABASA of Loudon County, Tennessee #USA GOV  
#DOWN

#UCC  
#CCA  
#KNT  
#SCA  
#GHOST

IN THE NAME OF "ALLAH"

\*\*\*\*\*

#UCC / CALIPHATE HACKERS DIVISION  
DATABASA of Loudon County, Tennessee #USA GOV  
#DOWN- SYSTEM FAILED

=====

\*\*\*\*\*

\*\*\*\*\*

\*\*\*\*\*

\*\*\*\*\*



#### IV. D. UCC POSTS NAMES AND ADDRESSES OF 3,600 PURPORTED NY CITIZENS

**Release Date:** April 21, 2016  
**Type of Target:** U.S. civilians  
**Platform of Distribution:** Telegram  
**Medium of Distribution:** Link to a document on pasting site (removed within 48 hours)  
**Information Provided:** Full names, email addresses, street addresses, phone numbers, and neighborhoods of residency



The UCC posted a list of 3,602 names and addresses of purported “most important citizens of #NewYork and #Brooklyn,” stating “we want them dead.” The list was posted as a plain-text file.

Analysis of the data shows many, though not all, of the listings to be publicly-accessible via general directories on the Internet. Some listings appear to have come from various other sources like small businesses, while others appear outright fake or questionable in nature (i.e. spam). For instance, at least 300 of the entries simply listed email addresses with aseekart.com and yahone.com domains, neither of which appear to be real.

balabo3_xd@aseekart.com	jyner_mm	jyner_mm
norman-gx@yahone.com	garry-vf	garry-vf
balabo3_pr@aseekart.com	jyner_bc	jyner_bc
norman-wd@yahone.com	garry-hp	garry-hp
balabo3_vp@aseekart.com	jyner_lf	jyner_lf
balabo3_jc@aseekart.com	jyner_jo	jyner_jo
balabo3_vg@aseekart.com	jyner_bw	jyner_bw
norman-zu@yahone.com	garry-bw	garry-bw
norman-rg@yahone.com	garry-df	garry-df
norman-vm@yahone.com	garry-tx	garry-tx
norman-hn@yahone.com	garry-ah	garry-ah
balabo3_kb@aseekart.com	jyner_wz	jyner_wz
norman-nk@yahone.com	garry-mg	garry-mg
norman-zw@yahone.com	garry-yn	garry-yn
balabo3_rx@aseekart.com	jyner_ut	jyner_ut
norman-ni@yahone.com	garry-xa	garry-xa
norman-lp@yahone.com	garry-mj	garry-mj
balabo3_hb@aseekart.com	jyner_wa	jyner_wa

Screenshot of spam content

List of the most important citizens of #NewYork and #Brooklyn and some other cities  
 MORE THAN #3000 NAME

We Want Them #Dead  
 #Shut THEM Down

Despite this, further analysis of the information, along with media reports of FBI agents notifying people in New York City, confirmed at least some of the names and addresses listed to be accurate of real New York residents.

#### IV. E. UCC CLAIMS HACKING U.S. STATE DEPARTMENT

**Release Date:** April 24, 2016

**Type of Target:** Federal government employees

**Platform of Distribution:** Telegram

**Medium of Distribution:** Images containing text

**Information Provided:** Names, places of work, and phone numbers



The UCC claimed hacking the U.S. State Department and posted images containing alleged names, places of work, and phone numbers of 50 staff members as "wanted to be killed." Each staff member had their own respective image with their information listed. In the announcement, the UCC indicated that these names were the "first part."

While most of the staff named in the images are identified as working for the Department of State, others are identified as working for the following entities:

- Department of Commerce
- Department of Defense – Australia
- Department of Defense
- Department of Energy
- Department of Homeland Security
- Department of Health and Human Services
- Department of the Navy

#isola

Wanted to be killed



## IV. F. ISHD DISTRIBUTES LIST OF NAMES, ADDRESSES OF 76 ALLEGED U.S. MILITARY DRONE PERSONNEL

**Release Date:** May 2, 2016

**Type of Target:** U.S. military personnel

**Platform of Distribution:** Twitter

**Medium of Distribution:** Link to a PDF uploaded to a file-sharing website

**Information Provided:** Rank, full name, personal address, and a short description



ISHD [disseminated](#) a list of the names and addresses of 76 alleged U.S. military drone personnel and threatened to leak "secret intelligence" purportedly obtained from the Ministry of Defense in London. The information was uploaded in a PDF to a file-sharing website and disseminated on Twitter on May 2, following the removal of a previous post to a pasting site on April 30.

The PDF listed the rank, full name, personal address, and short description of each of 76 military members, claiming them all to be involved with U.S. drone operations in various capacities.



*Example of two personnel listed in PDF*

The PDF also included a lengthy introductory message describing the nature of leak, and called for lone wolf IS fighters in the U.S. to "kill them wherever they are" and commit other acts of violence against the personnel listed.

The message specifically called out personnel at the "Creech" and "Holloman" U.S. Air Force bases near Las Vegas, NV and Alamogordo, NM, respectively as the primary "pilots and sensor operators that attack the Islamic State."

The message further threatened to leak "secret intelligence" supposedly obtained by IS from the Ministry of Defense in London, UK, claiming that IS fighters have "infiltrated England and [the U.S.] online and off."

Many of the names and addresses on the list were found to be available via public directories. However, the information appeared to be manually compiled, as there no publicly accessible unified list of the personnel.

#### IV. G. UCC RELEASES SECOND PART OF DATA FROM ALLEGED U.S. STATE DEPARTMENT

**Release Date:** May 2, 2016

**Type of Target:** Federal government employees

**Platform of Distribution:** Telegram

**Medium of Distribution:** Images containing text

**Information Provided:** Names, places of work, and phone numbers



The UCC [released](#) the second part of data it claimed obtaining from a hack of the U.S. State Department, giving information on another 50 staff members as "wanted to be killed." Similar to the first set released on April 24, the information came in the form of 50 images, each dedicated to an individual staff member, via a UCC-affiliated Telegram channel.

Additionally, the group posted an image with the text:

*Watch your windows very well  
The #FBI can't help you  
We will drink from your blood*

While the first list contained staff working in other U.S. government departments, this release was for the State Department alone. Analysis of the data showed that a minority of the information appeared to be publicly-accessible online and pertaining the U.S. State Department personnel, but the vast majority was not public or confirmed as genuine.

On May 17, the UCC further threatened to release yet another "Part 3" of the alleged State Department hack, stating, "We will kill you all." Though the group claimed the third part of the list would come "soon," it has not been released at the time of writing this report.





## IV. H. UCC POSTS NAMES, ADDRESSES OF 1,500 PURPORTED TEXAS RESIDENTS

**Release Date:** May 2, 2016

**Type of Target:** U.S. citizens

**Platform of Distribution:** Telegram

**Medium of Distribution:** Document uploaded to a pasting site (still available)

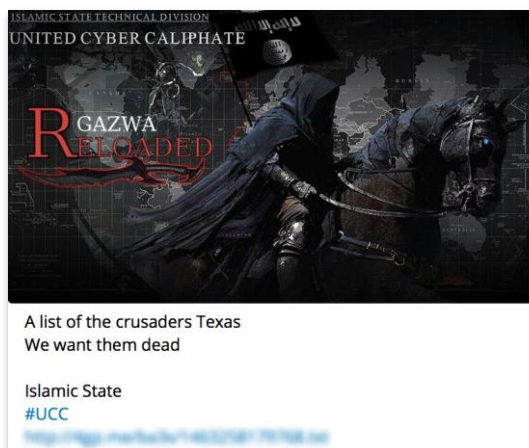
**Information Provided:** Full names, email addresses, personal addresses, phone numbers, and IP addresses



The UCC [posted](#) a list of 1,543 names, personal addresses, and IP addresses of purported "most important crusaders in #Texas" as "wanted to be killed," stating, "shoot them down."

Similar to the release of information about 3,600 alleged New York residents, analysis of the data shows many, though not all, of the listings to be publicly-accessible via general directories on the Internet. Some listings appear to have come from various other sources like small businesses, while others appear outright fake or questionable in nature (i.e. spam). Despite this, at least some of the names and addresses listed do appear to be accurate of real Texas residents.

On May 14, the UCC redistributed the list of Texans, stating, "We want them dead."





## V. CONCLUSION

The increasing emergence of pro-IS hacking groups and related kill lists mirrors activity happening elsewhere in the pro-IS community online. IS owes much of its growth to the grass-roots media machine run by its fighters and supporters. Given the power and ease of social media, along with the increasing ubiquity of Internet access and smart phones, every IS supporter can act as their own online media group, recruitment office, or fundraising organization. Likewise, every IS-supporting hacker can use their skills to serve the group's goals, whether they be a fighter or a supporter in non-combat zones.

It is important to note that these hacking groups exist within one largely unified online community, comprised of individuals and media groups which routinely vet and promote each other. Thus, while there appears to be no formal connection between the ISHD and partnered UCC and CCA, the groups may still coordinate releases outside of public view. Additionally, although there is currently not enough information available to conclude if hacking was involved in compiling the kill lists analyzed in this report, given some of the networking capabilities (e.g. the ISHD's coordination with Ardit Ferizi) and relatively sophisticated hacks (e.g. the CCA's takeover of a French TV broadcast) laid out in this report, hacking should be considered a possibility.

While the cyber-hacking context of these jihadi-purposed lists is relatively new, the only substantive difference between these releases and traditional hit lists is the designation of seemingly random civilian targets. Past kill lists have focused more on prominent political and economic targets, as well as recognized "blasphemers" of Islam. This shift in target selection shows a new method in serving a long-standing function of IS and other jihadi groups: instill widespread fear into governments and the public. The seemingly random selection of these lists, combined with their sizes (multiple of which exceeding 1,000 names), can be seen as a new and effective way of instilling such fear and perpetuating IS' terrorist methodology. As IS spokesman Abu Muhammad al-'Adnani stated in a September 2014 speech, Muslims should kill any non-Muslim living in countries warring with the group, with no distinction of "whether he is civilian or military."

***IS SPOKESMAN ABU  
MUHAMMAD AL - 'ADNANI: KILL  
NON-MUSLIMS IN WARRING  
COUNTRIES "WHETHER HE IS  
CIVILIAN OR MILITARY. "***

This open-ended target span understood, the kill lists discussed in this report appear to be adaptive applications of a larger, evolving terror threat.