The Revolution in Private Sector Intelligence

Richard Bejtlich

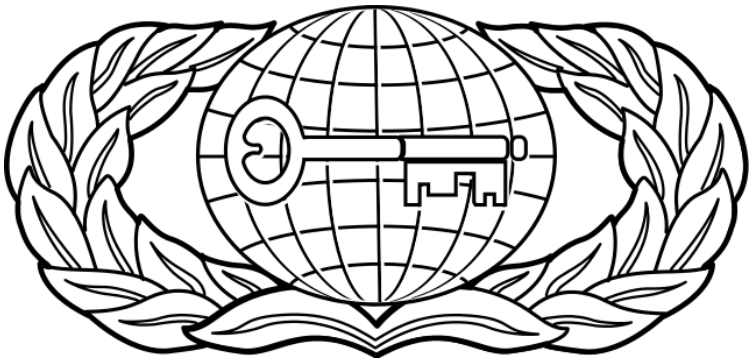
@taosecurity

4 February 2016

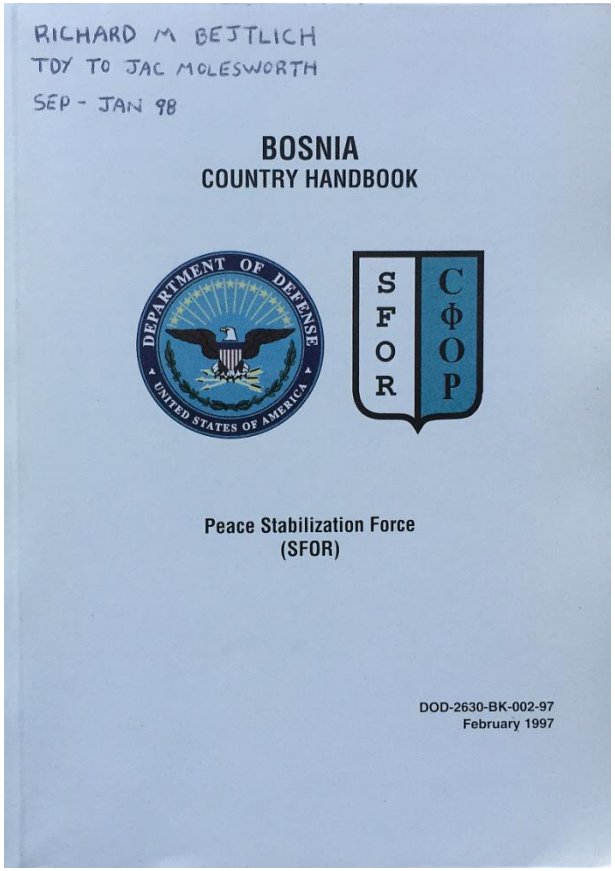
Bottom Line Up Front

- We are witnessing a revolution in intelligence capabilities in the private sector, powered by:
  - Imagery from commercial satellites, drones, and smart phones
  - Experts trained by the military and government
  - Collaboration among ex-mil/gov and pure civilians
  - Private job opportunities for these professionals
  - Software, some in the cloud, that enables the above
- The revolution creates benefits and costs, and we haven't figured it all out yet.

Air Force Intelligence Officer Graduation, March 1997



Unclassified Information Provided to Intelligence Analysts in Fall 1997


RICHARD M BEJTLICH
TDY TO JAC MOLESWORTH
SEP - JAN 98

BOSNIA
COUNTRY HANDBOOK

Peace Stabilization Force
(SFOR)

DOD-2630-BK-002-97
February 1997


SECTION 1

THE GENERAL FRAMEWORK AGREEMENT ON PEACE IN BOSNIA AND HERZEGOVINA

(THE DAYTON PEACE AGREEMENT)

Summary of the General Framework Agreement 1-1


SECTION 11
FWF INFANTRY WEAPONS
AND NIGHT VISION DEVICES

44-mm M57 Antitank Grenade Launcher

The M57 grenade launcher is a handheld, recoilless, smoothbore, muzzle-loaded (reloadable), percussion fired, 44-mm antitank weapon. Only one type of service grenade is used with the M57 launcher: the fin-stabilized Model 57 HEAT round. A steel strip formed to fit the shoulder is welded to the bottom of launchers of recent manufacture to provide better aiming stability.

Recognition Features

- Steel cylinder open at both ends.
- Two notches cut in muzzle face.
- Breech end of barrel flared.
- Bipod attached to launcher barrel.

Technical Data

Ammunition type:	HEAT
Maximum effective range:	200 m
Rate of fire:	5 rd/min
Night vision equipment:	None
Penetration:	320-mm RHA

FWF

11-1

Information Warfare Against Serbian Radio Television, 1 October 1997

Hill 619, Duga Njiva, Republika Srpska, Bosnia and Herzegovina

DISTRIBUTION A:
Approved for public release; distribution is unlimited.

Document created: 15 March 99
Air & Space Power Chronicles

Physical Attack Information Operations in Bosnia: Counterinformation in a Peace Enforcement Environment

by

Arthur N. Tulak, MAJ, USA
Military Analyst, Center for Army Lessons Learned

The United States Air Force recently published its Information Operations (IO) doctrine as Air Force Doctrine Document 2-5, *Information Operations*, on 5 August 1998. The document states that Air Force IO doctrine applies "across the range of military operations from peace to war."[1]

The components of Air Force IO are *counterinformation (CI)* and its two subsets of *offensive counterinformation (OCI)* and *defensive counterinformation (DCI)*. Counterinformation "seeks to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force [or adversary]."[2] US Forces apply counterinformation operations to establish information superiority through control of the information realm. *Information Superiority* is "the degree of dominance that allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition."[3] Air Force doctrine recognizes that "CI operations can include support of military operations other than war [MOOTW]," such as peace operations.[4] Accordingly, Air Force IO doctrine applies to Military Operations Other Than War (MOOTW) such as the NATO-led peace operations in Bosnia-Herzegovina: Operations Joint Endeavor, Joint Guard, and Joint Forge.

Counterinformation comprises both offensive counterinformation and defensive counterinformation IO activities. Offensive Counterinformation "includes actions taken to control the information environment. OCI operations are designed to *limit, degrade, disrupt or destroy* adversary information capabilities information systems."[5]

The five components of OCI are:

1. Psychological Operations (PSYOP)
2. Electronic Warfare (EW)
3. Military Deception
4. Info Attack
5. Physical Attack

A peace operation information campaign will employ all five of these components to shape the battlespace. Through offensive counterinformation operations, the peace operations force can target such things as adversary leadership, decision making and C^2, with the goal of controlling adversary decision process tempo, and attack the adversary's centers of gravity through non-lethal means in order to:

Ref: http://www.iwar.org.uk/iwar/resources/airchronicles/tulak.htm

Watching Vessels Pass through Bosphorus

BOSPHORUS NAVAL NEWS

GO

HOME | ABOUT ME | FOREIGN WARSHIP ON BOSPHORUS | POSTS | COMMENTS

AMPHIBIOUS | AUXILIARIES | COAST GUARD | CORVETTES | FRIGATES | MINE WARFARE | NAVAL AVIATION | PATROL CRAFT | SUBMARINES

← TCG Bayraktar To Be Lauched on 3rd October 2015 | Turkish LPD Project Reached Important Milestone →

Foreign Warship On Bosphorus 2015 (Part 43)

1 OCT 2015 | 6 COMMENTS

Russian Alligator class large landing ship *Nikolay Filchenkov* making her south bound passage through Istanbul, again with much cargo on her deck. Photo: Yörük Işık. Used with permission.

Welcome On Board!

Archives

Select Month

Email Subscription

Enter your email address to subscribe to this blog and receive notifications of new posts by email.

Join 4,348 other followers

Enter your email address

Sign me up!

Twitter

@Millermena @Interpreter_Mag Russia must be running out of targets in non-ISIS areas. 40 minutes ago

RT @Metin4020: My analysis about the evolution of clashes in Turkey: 'Is Turkey on the verge of civil war?' almon.co/2kaq via @... 1 hour ago

RT @Ata_Umurbey: Yarından itibaren Meteoroloji'den Marmara ve Kuzey Ege için 'Kuvvetli fırtına' uyarısı!.. denizhaber.com.tr/meteorolojiden... 3 hours ago

@hepdurgunsu @decider What about the Radicalization of Anakin Skywalker? 9 hours ago

RT @Yoruksik: BlackSeaFleet #ЧМФ Черноморский Флот steals my picture & distributes as their own pic

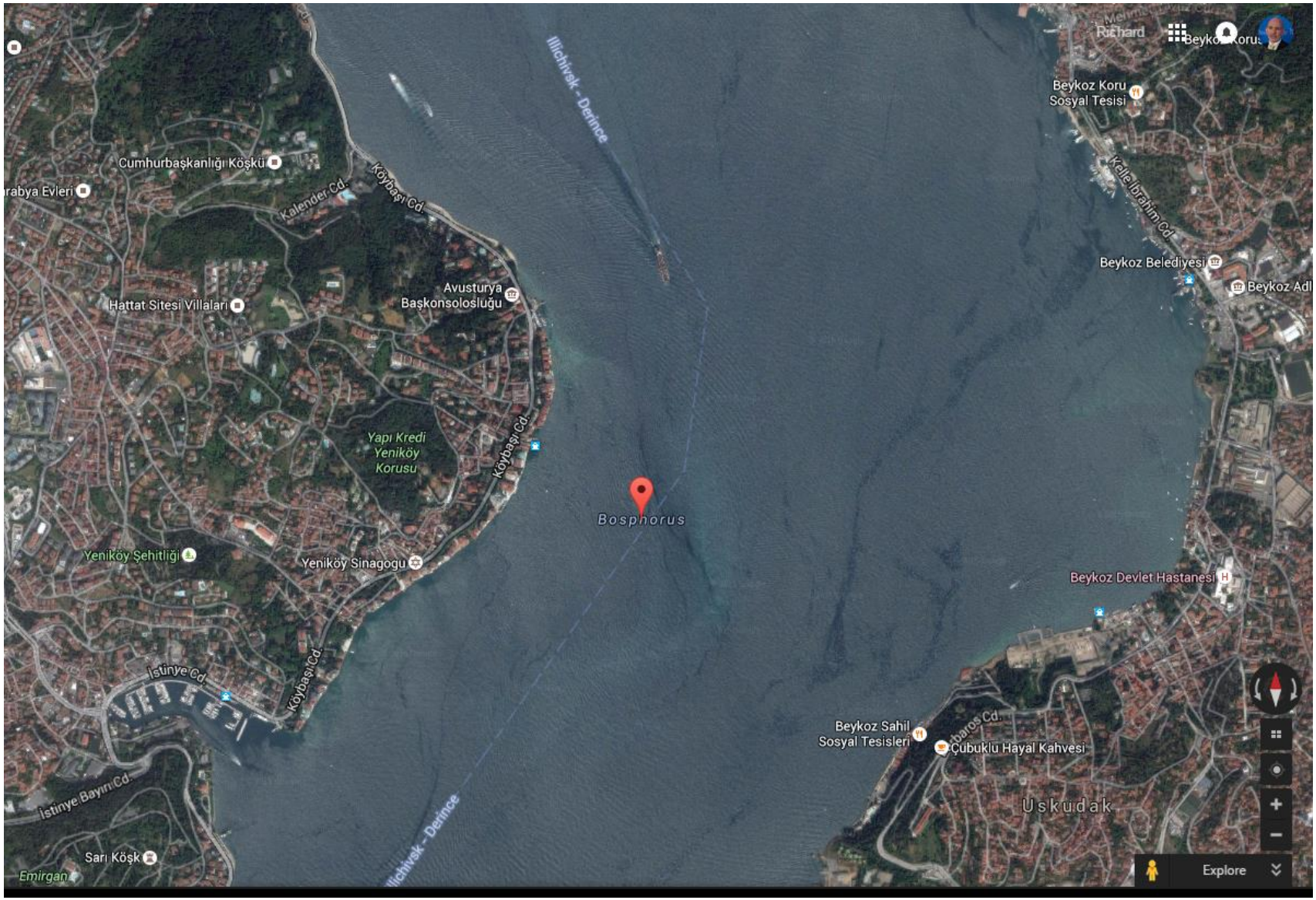
Last week we have saw a drastic increase in Russian warships movements through Turkish Straits.

One ship *Alexander Otrakovski* returned to the Black Sea, while 6 other warships *R-109, Ladny, Moskva, Saratov, Nikolay Filchenkov and KIL-158* made their southbound passage. The landings ship are on their cargo delivery missions whereas the larger warships are going to take part in a naval exercise around Cyprus, on 30 September 2015.

Date	Number	Name	Direction	Nationality
27.9.2015		KIL-158	Southbound	Russia
27.9.2015	152	Nikolay Filchenkov	Southbound	Russia
26.9.2015	150	Saratov	Southbound	Russia
25.9.2015	121	Moskva	Southbound	Russia
24.9.2015	801	Ladny	Southbound	Russia
24.9.2015	952	R-109	Southbound	Russia
24.9.2015	31	Alexander Otrakovski	Northbound	Russia
22.9.2015	151	Azov	Northbound	Russia
22.9.2015	158	Tsezar Kunikov	Northbound	Russia
21.9.2015	142	Novocharkassk	Southbound	Russia
20.9.2015		Donuzlav	Southbound	Russia
19.9.2015	810	Smetlivy	Southbound	Russia
19.9.2015		KIL-158	Northbound	Russia
17.9.2015	150	Saratov	Northbound	Russia
17.9.2015		Sayany	Northbound	Russia
16.9.2015		Novorossiysk	Northbound	Russia
15.9.2015	031	Alexander Otrakovski	Southbound	Russia
14.9.2015	151	Azov	Southbound	Russia
14.9.2015	158	Tsezar Kunikov	Southbound	Russia
13.9.2015	75	USS Donald Cook	Southbound	USA
10.9.2015	152	Nikolay Filchenkov	Southbound	Russia
9.9.2015		KIL-158	Southbound	Russia
7.9.2015	150	Saratov	Southbound	Russia
4.9.2015	210	Smolny	Southbound	Russia
3.9.2015	130	Korolev	Southbound	Russia
3.9.2015	142	Novocharkassk	Southbound	Russia

Ref: http://turkishnavy.net/2015/10/01/foreign-warship-on-bosphorus-2015-part-43/

Bosphorus?



Ref: Google Maps

Bosphorus!

Ref: Google Maps

Google Earth Imagery of Hill 619, Duga Njiva 2007-2012

22 Sep 2007

17 Apr 2011

15 Sep 2011

17 Aug 2012

Ref: Google Maps

CSIS Tracking Land Reclamation Activities in South China Sea

Ref: https://www.washingtonpost.com/graphics/world/south-china-sea/ and http://amti.csis.org/

38 North Project Tracking North Korean Economic Activity via Satellite Imagery

Close up of the new complex (before and after).

(March 12, 2015; Google Earth)

(September 2, 2015; Google Earth)

New bridge construction that will improve transportation between Rason and China.

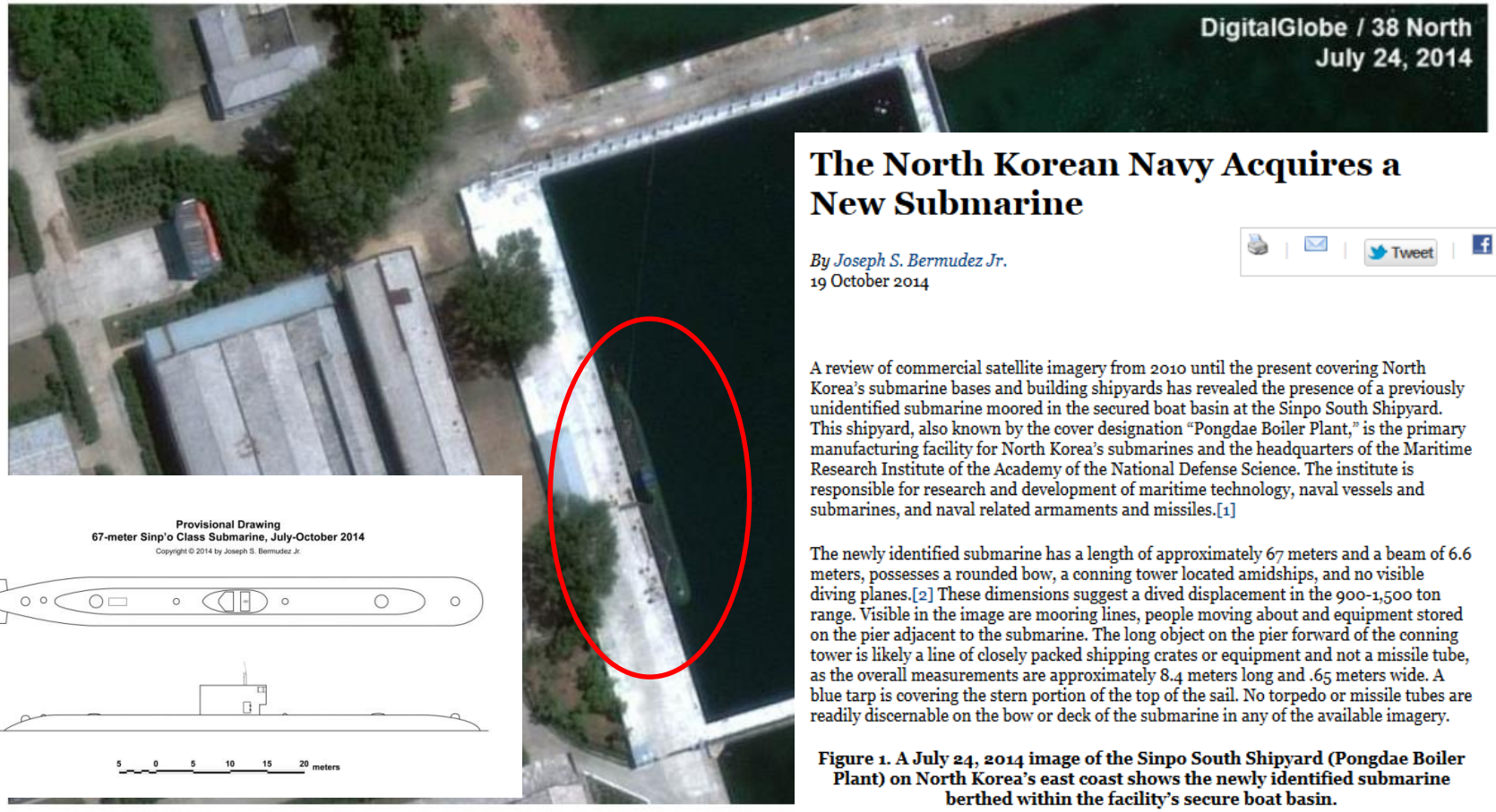
(September 15, 2013; Google Earth)

(September 6, 2015; Google Earth)

Ref: http://38north.org/wp-content/uploads/2015/11/38-North-SEZ-Plans-v-Progress-112315.pdf

38 North Project Identifies New North Korean Submarine

← The North Korean Navy Acquires a New Submarine



The North Korean Navy Acquires a New Submarine

Tweet

By Joseph S. Bermudez Jr.
19 October 2014

A review of commercial satellite imagery from 2010 until the present covering North Korea's submarine bases and building shipyards has revealed the presence of a previously unidentified submarine moored in the secured boat basin at the Sinpo South Shipyard. This shipyard, also known by the cover designation "Pongdae Boiler Plant," is the primary manufacturing facility for North Korea's submarines and the headquarters of the Maritime Research Institute of the Academy of the National Defense Science. The institute is responsible for research and development of maritime technology, naval vessels and submarines, and naval related armaments and missiles.[1]

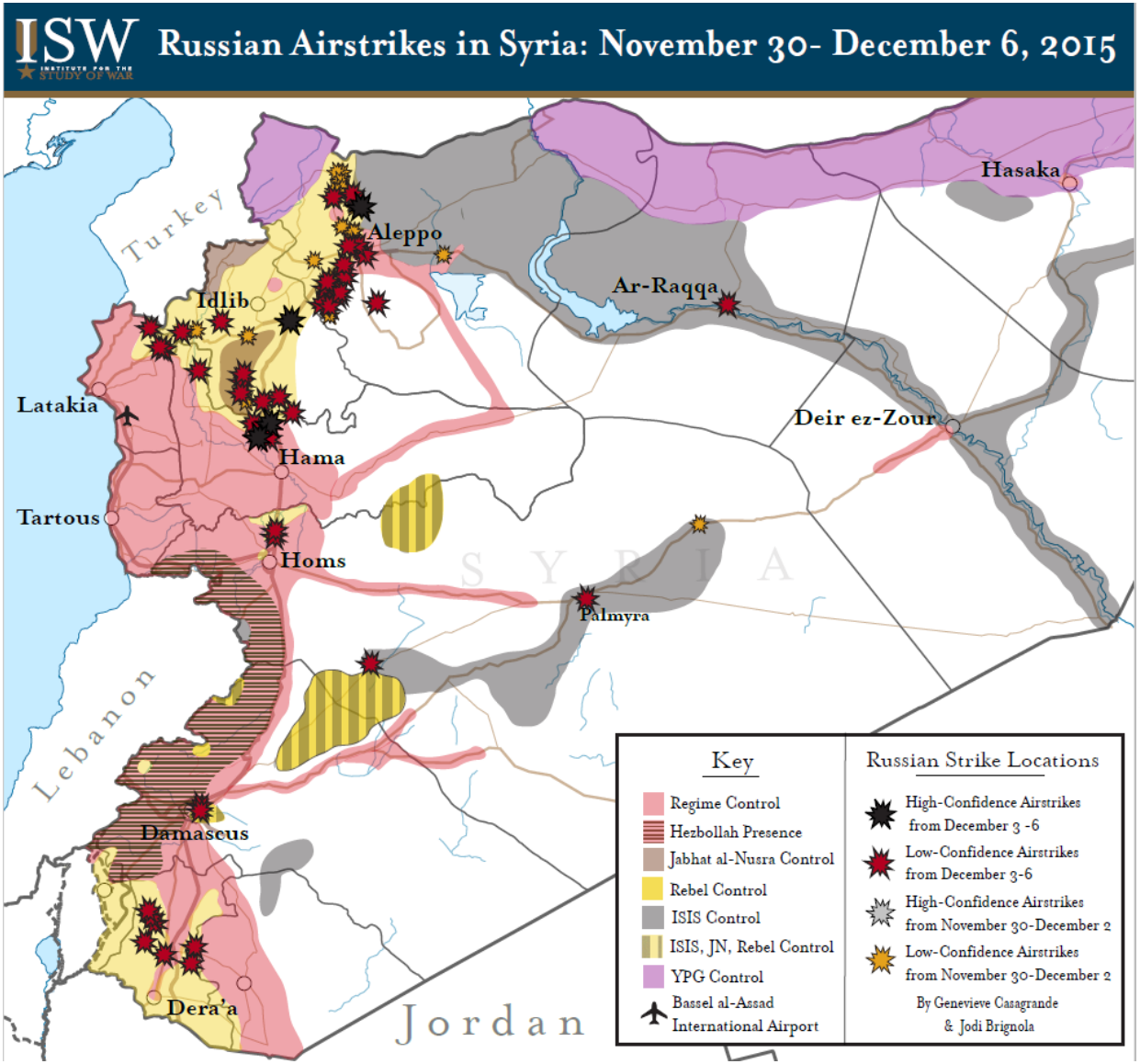
The newly identified submarine has a length of approximately 67 meters and a beam of 6.6 meters, possesses a rounded bow, a conning tower located amidships, and no visible diving planes.[2] These dimensions suggest a dived displacement in the 900-1,500 ton range. Visible in the image are mooring lines, people moving about and equipment stored on the pier adjacent to the submarine. The long object on the pier forward of the conning tower is likely a line of closely packed shipping crates or equipment and not a missile tube, as the overall measurements are approximately 8.4 meters long and .65 meters wide. A blue tarp is covering the stern portion of the top of the sail. No torpedo or missile tubes are readily discernable on the bow or deck of the submarine in any of the available imagery.

Figure 1. A July 24, 2014 image of the Sinpo South Shipyard (Pongdae Boiler Plant) on North Korea's east coast shows the newly identified submarine berthed within the facility's secure boat basin.

Figure 1. An image of the Sinpo South Shipyard (Bongdae Boiler Plant) on the east coast shows the newly identified submarine berthed within the facility's secure boat basin.
Return to the article: The North Korean Navy Acquires a New Submarine

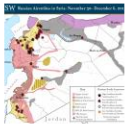
Ref: http://38north.org/2014/10/jbermudez101914/

Reports on Russian Air Strikes in Syria



RUSSIAN AIRSTRIKES IN SYRIA: NOVEMBER 30 - DECEMBER 6, 2015

Dec 8, 2015 - Genevieve Casagrande



Download the PDF

Russia resumed its air campaign in Southern Syria in support of regime ground operations against the FSA-affiliated Southern Front from December 3-6. Russia's renewed effort follows a December 3 declaration by FSA-affiliated Southern Front factions, including tribal fighters who claim to receive funding from Jordan, of a new offensive to seize the regime-held Judayyah artillery battalion in the northwestern countryside of Dera'a province. Russian airstrikes targeted areas along the nearby frontline surrounding the battalion, an area primarily held by Southern Front-affiliated factions. The shift comes just two weeks after Russian President Vladimir Putin vowed to avoid hitting "healthy," non-terrorist rebel groups in Syria and to focus air operations against ISIS. While talks between members of the Syrian opposition and the Syrian regime are tentatively scheduled for January 1, 2016, Russia's continued aggression makes the prospects of a mutually agreeable political transition unlikely.

The Syrian Foreign Ministry accused the U.S.-led coalition of conducting an airstrike against a regime military position in the town of Ayyash in Deir ez-Zour province on December 6 killing four Syrian Arab Army (SAA) soldiers and wounding thirteen others. The ministry sent a letter to the U.N. Security Council in protest of "flagrant aggression by the U.S.-led coalition forces." Operation Inherent Resolve Spokesman Colonel Steve Warren denied that the Coalition carried out the attack, stressing that the nearest coalition strikes targeted an ISIS-held oil field 35 miles away from the incident. Anonymous Pentagon officials stated that radar data indicated that the bombing had been a 'friendly fire' incident committed by a Russian bomber. Local sources have previously reported on alleged Russian strikes against regime positions along frontlines in both Homs and Latakia Provinces.

The following graphic depicts ISW's assessment of Russian airstrike and cruise missile locations based on reports from local Syrian activist networks, Syrian state-run media, and statements by Russian and Western officials. This map represents locations targeted by Russia's air campaign, rather than the number of individual strikes or sorties.

High-Confidence reporting. ISW places high confidence in reports corroborated both by official government statements reported through credible channels and documentation from rebel factions or activist networks on the ground in Syria deemed to be credible.

Low-Confidence reporting. ISW places low confidence in secondary sources that have not been confirmed or sources deemed likely to contain disinformation.

Ref:
http://www.understandingwar.org/backgrounder/russian-airstrikes-syria-november-30-december-6-2015

AEI Critical Threats Project Comments on AllSource Analysis Reporting of Russian Aircraft in Syria

ALLSOURCE ANALYSIS

The Russo-Iranian Military Coalition in Syria may be Deepening

By Frederick W. Kagan, Marie Donovan, Paul Bucala
December 14, 2015

The Russo-Iranian military coalition in Syria may be deeper than many have believed. The Iranian armed forces appear to be allowing Russian aircraft to use their military airfields in support of combat operations over Syria. This development is remarkable: Iran is one of the most virulently anti-colonial regimes in the world, and yet it is allowing a former colonial power that had partitioned Persia with Great Britain to place military forces on its territory. But Russia likely requires access to an airfield in Iran to support its military operations in the region, and Tehran seems willing to permit it. Contrary to Western analysts' arguments that Russia is marginalizing Iran in Syria or even driving it out, Russia appears to be more dependent militarily on maintaining a strong relationship with Tehran than has been previously thought.

Iranian fighters have been escorting Russian bombers as they transit Iranian airspace for some time, as can be seen in a video filmed and released by the Russian air force (reported by *The Aviationist*). Military aviation specialist Babak Taghvaei reports (as cited by *The Aviationist*) that Russian Tu-95MS Bear, Tu-160 Blackjack, and Tu-22M Backfire bombers have flown a southwesterly path through Iranian airspace since late November on their way to missions against rebel and Islamic state forces in Syria, flying southwest of Tehran, passing Esfahan and Ahvaz, and crossing over the Iraqi border north of Basra. Satellite imagery recently obtained and analyzed by AllSource Analysis now shows that advanced Russian combat aircraft have used Iranian Air Force bases to stage on the way to or from bombing runs in Syria at least once.

One such combat aircraft, a Russian Su-34 "Fullback" strike fighter, was seen on the main parking apron of Shahid Nojeh Air Base in the northwestern province of Hamedan, Iran on November 23, 2015 and remained there for at least two days. An Il-76 "Candid" transport aircraft arrived likely in the afternoon or evening of November 24. Both had departed by December 5, according to AllSource analysts.

Ref:
http://www.criticalthreats.org/russia/kagan-donovan-bucala-russo-iranian-coalition-in-syria-deepening-december-14-2015

Crowdsourcing Russian Reports of Airstrikes in Syria

Verifying Russian airstrikes in Syria with Silk, two months on

by: Eliot Higgins
Bellingcat
Date: December 6, 2015

5 mins

Recommend: 3

Sign in to save this article

Add to a pack

Share:

Tags: geolocation, syria, russia

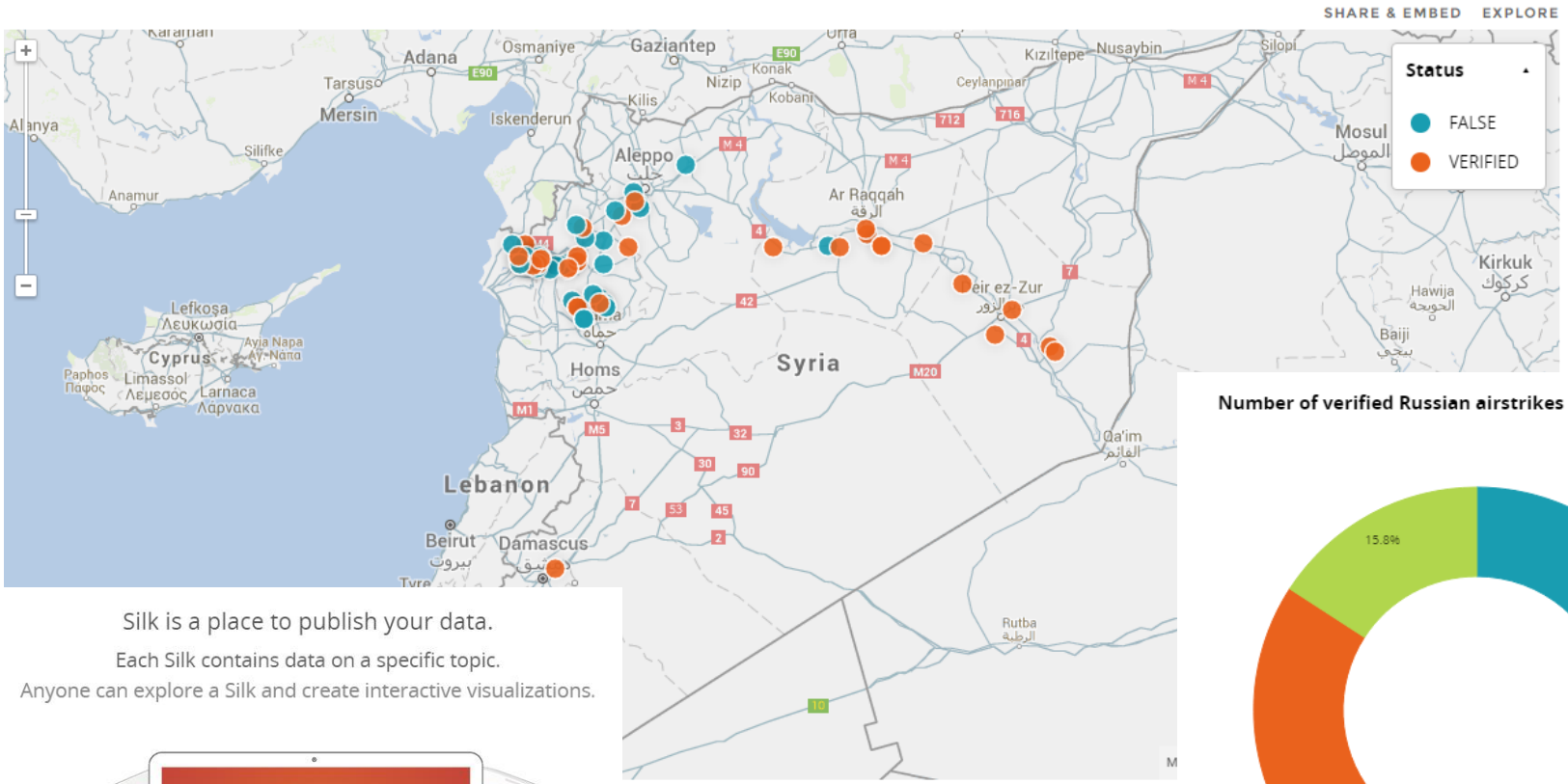
Bellingcat has been tracking and analysing videos of Russian airstrikes in Syria posted to an official YouTube channel. Results have been mixed.

Screenshot from a video posted to the YouTube channel of the Russian Ministry of Defense, allegedly showing an airstrike in Syria. It has yet to be verified by the Bellingcat team.

Ref: http://firstdraftnews.com/verifying-russian-airstrikes-in-syria-with-silk-two-months-on/

Results Show About 45% of Russian Gov Claims Are False, 40% Are True, 15% Unconfirmed

Airstrikes mapped by actual location co-ordinates

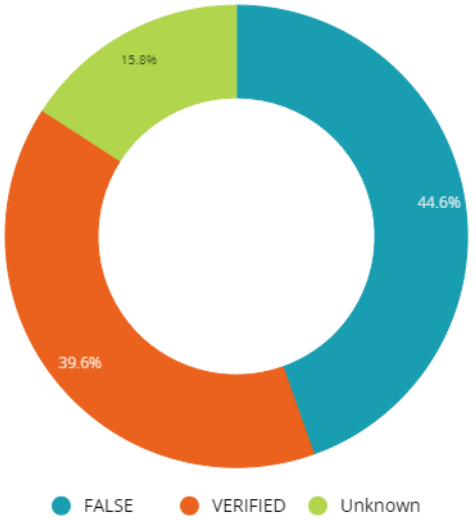


Silk is a place to publish your data.

Each Silk contains data on a specific topic.
Anyone can explore a Silk and create interactive visualizations.

Ref: https://russia-strikes-syria.silk.co/

Number of verified Russian airstrikes grouped by status



GWU Report on ISIS in America

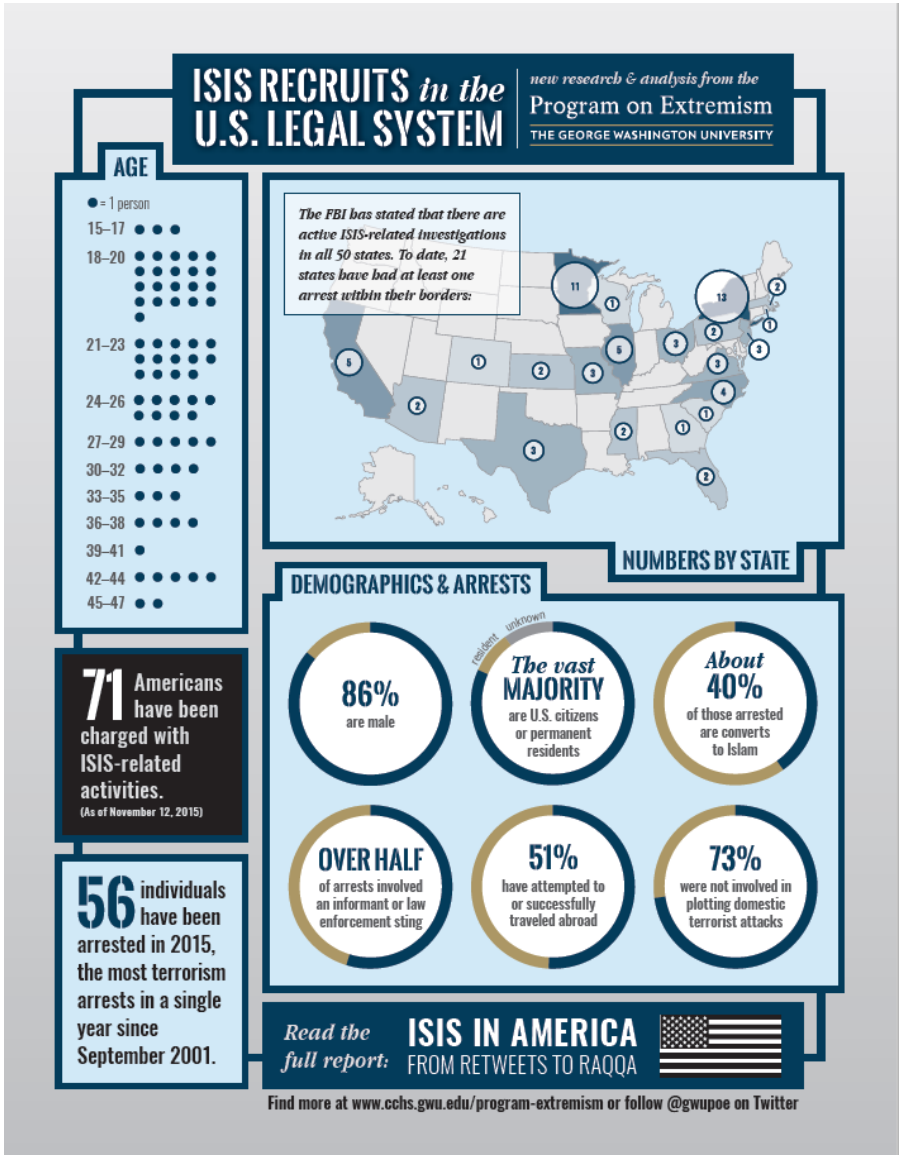
ISIS IN AMERICA

FROM RETWEETS TO RAQQA

Lorenzo Vidino and Seamus Hughes
December 2015

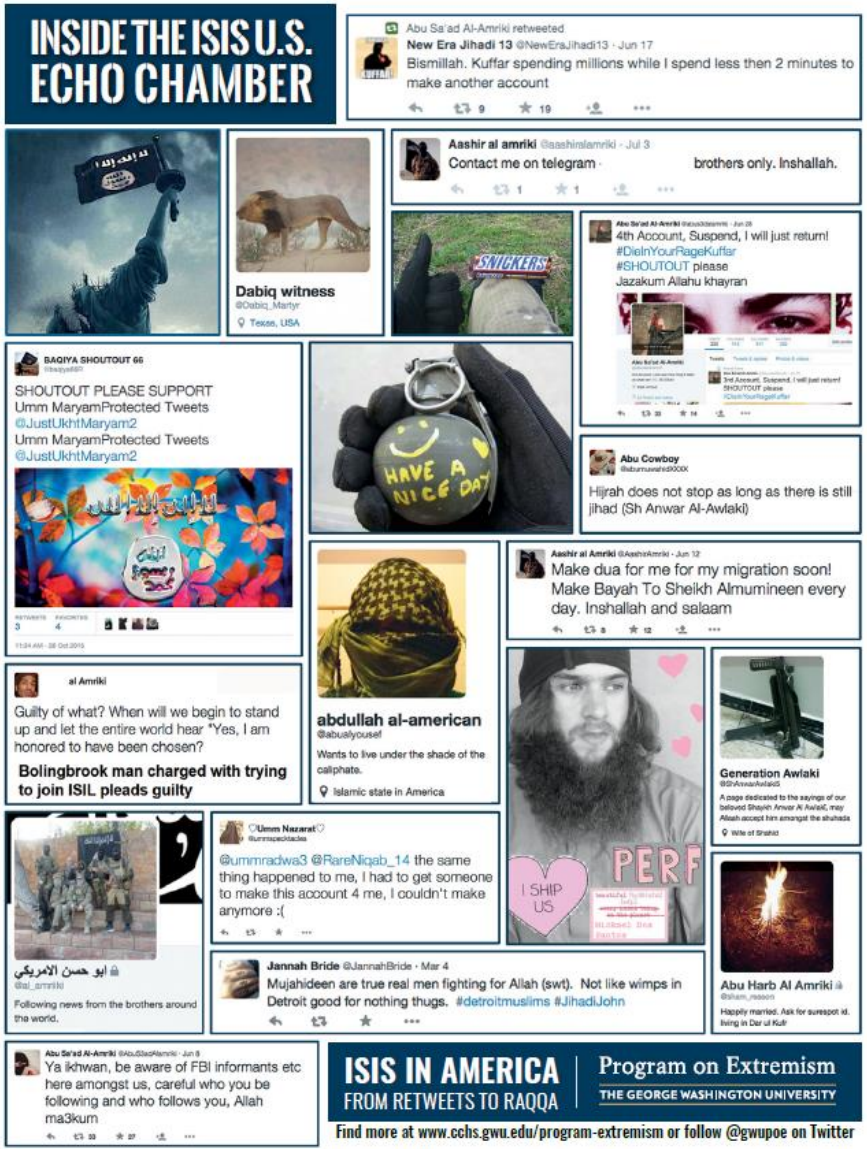
Program on Extremism
THE GEORGE WASHINGTON UNIVERSITY

The Program on Extremism reviewed more than 7,000 pages of legal documents detailing ISIS-related legal proceedings, including criminal complaints, indictments, affidavits, and courtroom transcripts. Supplemented by original research and interviews with prosecutors, reporters, and, in some select cases, families of the charged individuals, the Program developed a snapshot of the 71 individuals who have been charged for various ISIS-related activities.



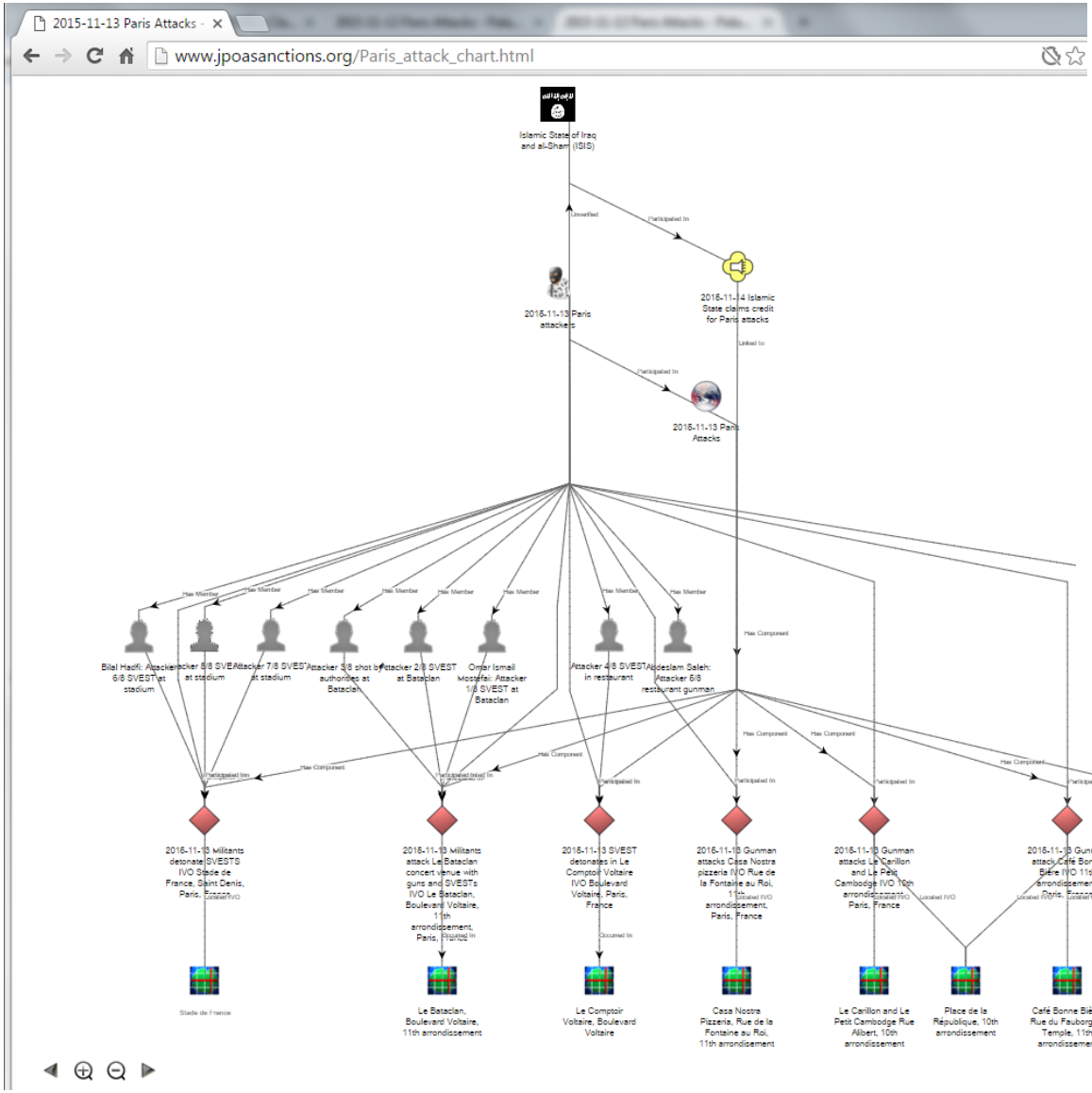
Ref: http://cchs.gwu.edu/isis-in-america

GWU Report on ISIS in America



Ref: http://cchs.gwu.edu/isis-in-america

Fast Analysis: Network Graph of IS Paris Attack



Network Graph of ISIS's Claimed Attacks in Paris

By Emily Estelle, Harleen Gambhir, Katie Menoche
November 15, 2015

ISIS's claimed attacks in Paris on November 13 mark the organization's most sophisticated assault in the West to date. This interactive graphic depicts the individuals, events and locations directly linked to the Paris attacks. Eight attackers in three coordinated teams attacked six locations in Paris including the Stade de France sports stadium and the Bataclan art center with AK-47s, grenades, and SVESTs. The assailants aimed to maximize civilian casualties, taking concert attendees hostage and attempting to launch a suicide attack in a soccer stadium. The total casualties inflicted by ISIS as of November 15 are 129 dead and 352 wounded, the second most deadly terrorist attack in the West since 9/11.

The eight attackers depicted in ISW and CTP's graphic likely enjoyed the support of a broader logistics and planning network active in multiple countries. Initial reports suggest that the attackers included French nationals living in France and Belgium as well as Syrian passport holders, one having entered Europe through a Syrian refugee camp on the Greek island of Leros. ISW and CTP will publish updates to this graph as the broader extent of ISIS's terrorist network in Europe becomes known.

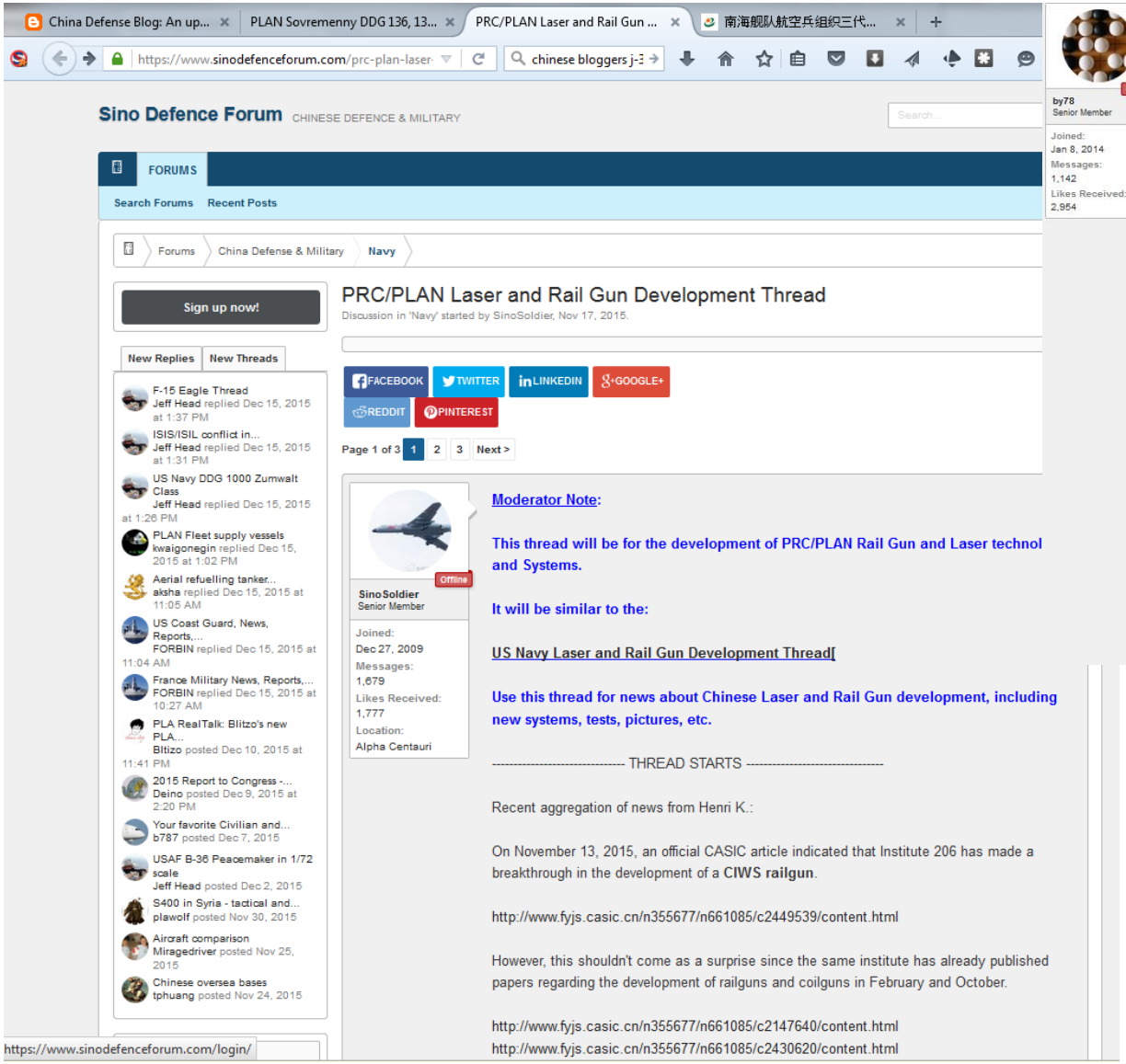
The Paris attacks do not represent a shift in ISIS's strategy. Rather, they represent a major success in ISIS's announced plans to encourage, resource, and direct terror attacks in the West. ISIS seeks to punish Western and regional adversaries acting against it in Iraq and Syria. ISIS also aims polarize communities in the U.S. and Europe by inspiring fear and suspicion. Terrorist attacks may sharpen social cleavages in Europe and increase the strain upon refugees in a way that supports ISIS's aim. ISIS-linked operatives have attempted attacks in numerous European countries, including France, since January 2015. ISIS will likely continue using its foreign fighter networks to plot attacks in Europe and the wider world.

ISIS will continue to export lethal capabilities from Iraq and Syria to foreign operatives plotting against the West. ISIS-linked individuals likely built the SVESTs deployed in Paris while in Europe, after receiving training in Iraq and Syria. This transfer of military knowledge undermines anti-ISIS strategies intended to contain ISIS within Iraq and Syria. The organization's global network is active, far-reaching, and expanding while ISIS sustains tactical losses within Iraq and Syria.

This graph was produced with the Institute for the Study of War.

Ref:
http://www.criticalthreats.org/other/ctp-isw-network-graph-isis-claimed-attacks-in-paris-november-15-2015

China Laser and Rail Gun Development Thread Shows Expertise and Collaboration



Ref: https://www.sinodefenceforum.com/prc-plan-laser-and-rail-gun-development-thread.t7906/

Physical World Attribution: “Little Green Men”

Little green men (2014 Crimean crisis)

From Wikipedia, the free encyclopedia

For other uses, see Little Green Men (disambiguation).

Little green men (Russian: зелёные человечки, Ukrainian: зелені чоловічки), in Russia **Polite People** (Russian: вежливые люди, Ukrainian: ввічливі люди),[1][2][3][4][5][6] is a colloquial expression referring to masked unmarked soldiers in green army uniforms wielding Russian military weapons and equipment within Ukraine. It was first used during the 2014 Crimean crisis, when said soldiers occupied and blockaded the Simferopol International Airport, most military bases in Crimea[2] and the parliament in Simferopol.

Retired Russian Admiral Igor Kasatonov has revealed that the little green men belonged to the army Spetsnaz and said that according to his information the Russian troop deployment in Crimea included six helicopter landings and three landings of IL-76 with 500 people.[7]

Ref: https://en.wikipedia.org/wiki/Little_green_men_%282014_Crimean_crisis%29

Atlantic Council Report on Russia vs Ukraine

Ref: http://www.atlanticcouncil.org/images/publications/Hiding_in_Plain_Sight/HPS_English.pdf

Report on Identities, Deployment, and Deaths of Russian Soldiers Fighting in Ukraine

Section 3. Russian Soldiers in Ukraine

The Russian military is sending its soldiers across the border to mix with Russian-instigated separatist forces in Ukraine.

Once in eastern Ukraine, these soldiers are no longer considered Russian; rather they are told to refer to themselves as "local defense forces," aiding the separatist soldiers with additional manpower and Russian equipment. In addition to Bato Dambayev, two more soldiers, Anton Tumanov and Leonid Kichatkin, profiled in this report represent the routine process of how Russian soldiers train in "exercises" near the Ukrainian border, cross covertly into Ukraine, and fight against Ukrainian soldiers.

Soldier Profile 2. Anton Tumanov

Russian 18th Motorized Brigade, Unit 27777

Tumanov was sent to Ukraine while on active duty in the Russian military in August 2014. He perished on August 13, 2014, in Snezhnoe, Ukraine after crossing the border on August 11, 2014.

Life before the War

Prior to joining the Russian military, Anton frequently voiced his concerns about the state of the local economy in his hometown of Kozmodemyansk, Russia. He saw no alternative to joining the military, even knowing the danger of being sent to fight in eastern Ukraine. As his mother said:

> *Where can you work here in Kozmodemyansk? There are only two factories left. In May he told me "Mom, I'm going to the army." I tried to persuade him to wait with that idea. "God forbid, they'll send you to Ukraine," I told him," she recalls. "He told me the army wouldn't be sent to Ukraine. He said, "I need money. I'm not going to a war. I'm going to a job. There is no other job anyway."*[96]

His mother did not want him to join the army, but Anton went nonetheless.[97]

Training for Combat

While at a training camp near the Ukrainian border, Anton's commanders gave the order on August 11, 2014: turn in your phones, take off identifying features from your uniform, mask the unique markers on military equipment, and cross into Ukraine. Those who refused were "insulted and threatened by the commanders."[98] The twenty-year-old entered Ukraine with over a thousand others and a large column of military equipment, and his smaller group arrived in Snezhnoe late on August 12, 2014.

96 *Novaya Gazeta*, http://www.novayagazeta.ru/society/65075.html (in Russian).
97 Ibid.
98 Ibid.

Photo: Tumanov with his fiancée Natasha Chernova in June 2014, before he left for service.[99]
Source: Tumanov's VKontakte page.
Coordinates: 56.3453311, 46.5708947 (estimated).

Photo: Tumanov on the grounds of his camp near the Ukraine border before his deployment to Ukraine.
Source: Tumanov's VKontakte page.[100]
Coordinates: 48.320520, 40.099180.

99 Chernova told *Novaya Gazeta* and Anton talked to her in late July, in which he said that he would soon be leaving for Ukraine to fight "in the role of opolchentsy," a term that refers to local separatist fighters in eastern Ukraine. See http://www.novayagazeta.ru/society/65075.html (in Russian).
100 VKontakte, https://vk.com/tyman_antoxa?z=photo140456238_334848101%2Fphotos140456238 (archived: https://archive.is/q0aZM).

Photo: Snezhnoe, Ukraine, August 13, 2014. The last known picture of the group before the deadly shelling. Robert Artyunyan (second from right) and Anton Tumanov (far right) died on August 13. Rolan Ramazanov, the soldier in the middle, shared this image online on August, 26, 2014.[101]
Source: Novaya Gazeta.[102]
Coordinates: 48.058296, 38.757780 (estimated).[103]

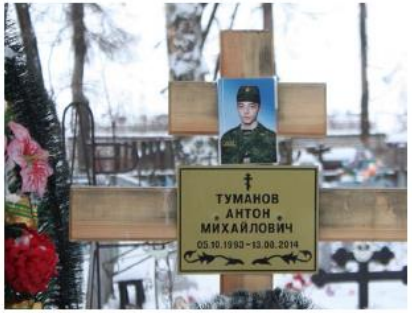


Photo: Tumanov's grave in his home town of Kozmodemyansk, four hundred miles east of Moscow, Russia.
Source: Tom Parfitt, *Telegraph.*[104]

101 The exact location of this photograph is unknown, but it was taken somewhere in Snezhnoe—likely at or near the Khimmash factory, where an artillery strike killed Anton. See *Novaya Gazeta*, http://www.novayagazeta.ru/storage/c/2014/09/01/1409580145_413509_31.jpg.
102 *Novaya Gazeta*, http://www.novayagazeta.ru/storage/c/2014/09/01/1409578904_547636_54.png.
103 Ibid.
104 Tom Parfitt, "Secret Dead of Russia's Undeclared War," *Telegraph*, December 27, 2014, http://telegraph.co.uk/news/worldnews/europe/russia/11314817/Secret-dead-of-Russias-undeclared-war.html.

Deployment to and Death in Snezhnoe

Anton Tumanov and his fellow unit member Robert Artyunyan documented their arrival in Snezhnoe on August 13—the same place where, twenty-seven days earlier, the Buk system that likely shot down MH17 was spotted hours before the crash.

Numerous eyewitnesses on August 13 report seeing a convoy moving through Torez and Snezhnoe, specifically noting a BTR-80 (an armored vehicle) and men with "white bands"[105] on their arms and legs. Not coincidentally, Tumanov and his fellow soldiers were photographed with white bands and a BTR-80a in Snezhnoe. Only hours after the photograph was taken, local social media reports and videos described how the Khimmash factory was hit by an artillery strike from the Ukrainian military.[106] This strike killed Tumanov and Artyunyan. Rolan Ramazanov, a Russian soldier from unit 27777 (pictured in middle of photograph) who survived the attack, described it to Reuters:

> *I was in the BTR. The hatches were open, and as a result—[I suffered] a concussion and minor loss of hearing. Robert and Anton were about two-three steps from the BTR [that I was in]. They just didn't manage to get away. Robert died on the spot. They gave medical help to Anton. He died on the operating table, said Rolan, having returned home to the Krasnodar Krai to recover from his injury.*[107]

Along with Artyunyan, Tumanov died on August 13, 2014 in Snezhnoe. He is buried in his hometown of Kozmodemyansk, Russia, over a thousand kilometers from Snezhnoe, Ukraine. According to the official documentation of his death, reported in the *Telegraph* report and elsewhere, Tumanov died "carrying out responsibilities of military service at a point of temporary deployment of military unit 27777."[108]

Soldier Profile 3. Leonid Kichatkin

Russian 76th Airborne Division, Unit 74268

Like Anton Tumanov, Leonid Kichatkin died in August 2014 while fighting in eastern Ukraine, under direct orders of his commanders in the Russian military. The authorities went to great lengths to cover up his death.

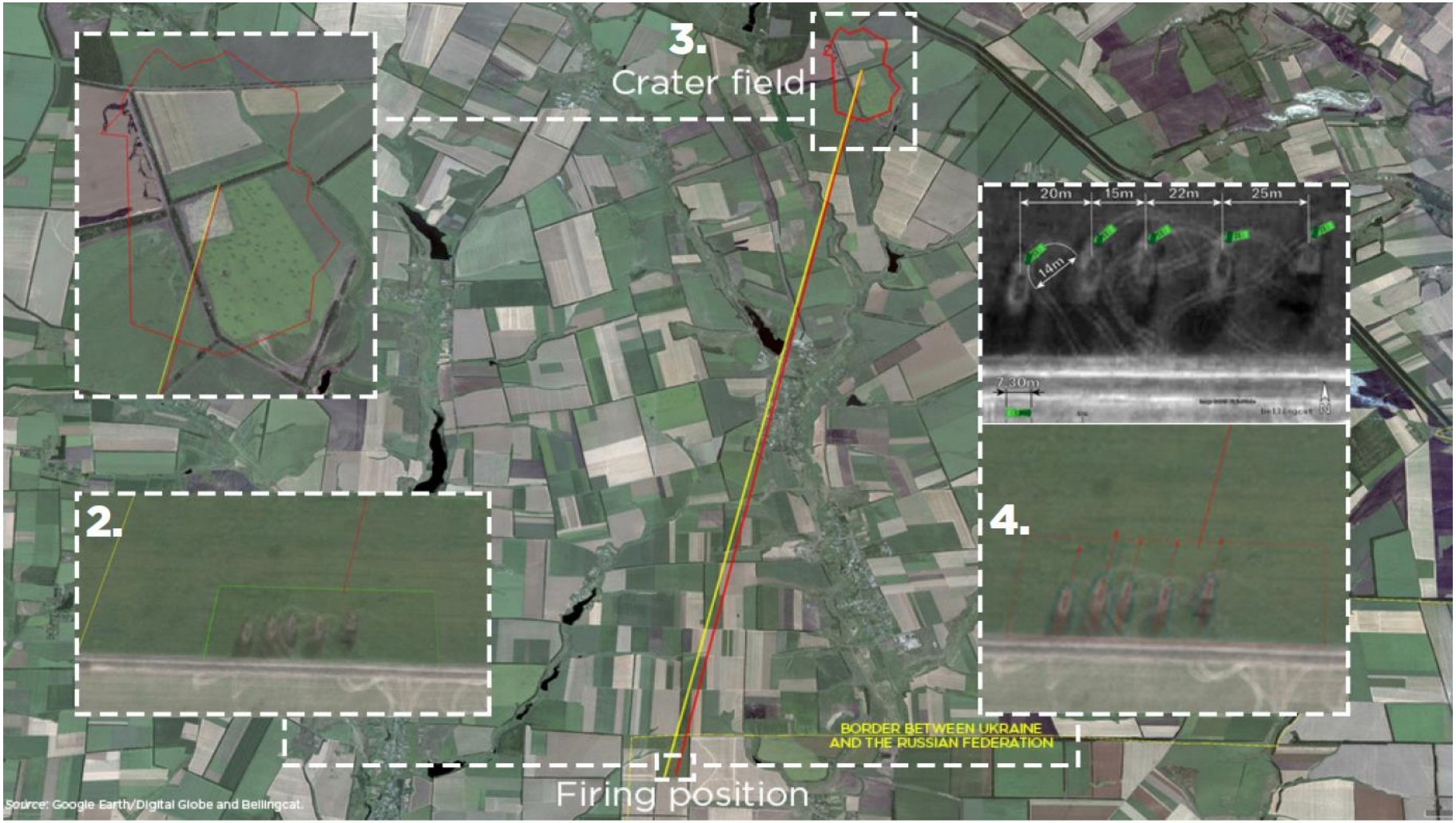
Before Ukraine

Leonid Kichatkin was a Sergeant in the Russian Airborne Troops. He lived with his wife, Oksana, and children in Pskov, where he was stationed for his military service. In late July 2014, Ukraine was close to defeating separatist forces as it retook territory, but the separatists were seemingly miraculously reinvigorated. In mid-August, Oksana would speak to her husband for the last time, as he and other Russian soldiers were ordered into Ukraine where they quickly stopped the Ukrainian counteroffensive.

105 Twitter, https://twitter.com/Dbnmjr/status/499578362428686336 (in Russian); https://archive.is/8XwoH (archived).
106 VKontakte, https://vk.com/liveuanet?w=wall-75493249_141%2Fe412e83adad6110ba6 (in Russian); VKontakte, https://vk.com/video115925565_169894607.
107 Reuters, http://ru.reuters.com/article/topNews/idRUKBN0H719A20140912 (in Russian).
108 Ibid.

Ref: http://www.atlanticcouncil.org/images/publications/Hiding_in_Plain_Sight/HPS_English.pdf

Crater and Burn Analysis to Determine Location of Firing Positions



Maps showing the average trajectory of craters measured at the Amvrosiivka impact site, the approximate direction of fire indicated by burn marks on the ground near Seleznev, and the position and size of multiple rocket launchers used during the attack based on the position of track marks at the launch site. *Source*: Satellite image from Google Earth/Digital Globe.

Ref: http://www.atlanticcouncil.org/images/publications/Hiding_in_Plain_Sight/HPS_English.pdf

Crater and Burn Analysis to Determine Location of Firing Positions

Example 1. The Amvrosiivka Attack, July 14, 2014

Coordinates: 47.764550, 38.513236.
Source: Google Earth/Digital Globe.

In a July 14, 2014 summary of the "anti-terrorist operation," Ukrainian media reported that an attack took place on positions of the Ukrainian armed forces in the vicinity of Amvrosiivka.[121] It was suspected that the origin of this attack was the territory of Russia.[122]

1. Satellite imagery from July 16, 2014, shows a corresponding extensive crater field south of Amvrosiivka. The observable direction of each of the 330 craters in this crater field were analyzed, and an average trajectory of these craters was calculated and determined to be 193.97°, i.e., from the south-south west (180° being due south).

2. When screening for possible firing positions from this trajectory, a firing position was found 14.6 kilometers from the crater field.

3. Burn marks are visible at this location on satellite map imagery from July 16, 2014 which is on Russian territory and approximately 750 meters from the border near the Russian village of Seleznev at the coordinates 47.63709, 38.469355.

4. The Amvrosiivka crater field is located south of the town at 47.76455, 38.513236. Satellite imagery from July 16 indicates a launch site coinciding in time with the report of the attacks at 47.63709, 38.469355.

Based on the markings at the launch site of the attack, it was possible to determine the type of multiple rocket launcher used (the BM-21 Grad/Tornado) and its position in relation to the damage done to the launch site.

The launch site north of Seleznev is showing clear burn marks from multiple rocket launches and track marks from the movement of vehicles in the area.

Burn marks at the site were used to determine the likely trajectory of the attack, and this matched the trajectory determined by the crater analysis.

121 "Anti-Terrorist Operation: Summary for July 14, 2014," InformNapalm, July 15, 2014, https://en.informnapalm.org/anti-terrorist-operation-summary-for-july-14-2014/, http://web.archive.org/web/20150210142924/.
122 Facebook, https://www.facebook.com/v.parasyuk/posts/675221185878989 (in Ukrainian) (https://archive.today/Z4NVR).

Ref: http://www.atlanticcouncil.org/images/publications/Hiding_in_Plain_Sight/HPS_English.pdf

Attribution: China's "Little Blue Men" Harass US Navy on Freedom of Navigation Mission

China's 'Little Blue Men' Take Navy's Place in Disputes

By Christopher P. Cavas 8:54 p.m. EST November 2, 2015

China using maritime militia to carry out its dirty work in seagoing confrontations

(Photo: US Navy)

CONNECT TWEET LINKEDIN COMMENT EMAIL MORE

WASHINGTON — When the US destroyer Lassen passed near a newly-built artificial island on Subi Reef in the South China Sea's Spratly Islands Oct. 27, it was already being escorted by several Chinese Navy warships. The US ship represented a challenge to China's attempt to create land and declare it and the surrounding areas sovereign territory.

The Chinese naval ships, reported a US Navy source, behaved professionally during the Lassen's transit. "They shadowed the Lassen but stayed at a safe distance."

But several smaller vessels, described by the source as merchant ships or fishing vessels, were more provocative, crossing the Lassen's bow and maneuvering around the destroyer even as they kept their distance.

"There were Chinese merchant vessels present that were not as demure as the Chinese Navy," the US Navy source said Oct. 30. "One came out of its anchorage in the island and crossed the destroyer's bow but at a safe distance, and the Lassen did not alter course as the merchant ship circled around."

Fishing vessels in the area added to shipping traffic in the immediate area, the source said. But the extra craft seem to have been present, the source noted, "because they anticipated the Lassen's transit."

GLOBAL ANALYSIS, ASIA-PACIFIC

IRREGULAR FORCES AT SEA: "NOT MERELY FISHERMEN—SHEDDING LIGHT ON CHINA'S MARITIME MILITIA"

NOVEMBER 2, 2015 ANDREW ERICKSON LEAVE A COMMENT

Ref: http://www.defensenews.com/story/defense/naval/2015/11/02/china-lassen-destroyer-spratly-islands-south-china-sea-andrew-erickson-naval-war-college-militia-coast-guard-navy-confrontation-territorial-dispute/75070058/

http://cimsec.org/new-cimsec-series-on-irregular-forces-at-sea-not-merely-fishermen-shedding-light-on-chinas-maritime-militia/19624

Attribution: Local Criminal and High Military Affairs

This video shows a burglar breaking into Dan's Wellness Pharmacy in Stafford for a 3rd time

NEWS

by Stafford Local on December 13, 2015 at 9:39 pm Leave a Comment

An independent pharmacy owner in Stafford hopes investigators can find out who keeps trying to break into his store.

A burglar tried to break into Dan's Wellness Pharmacy, located at 418 Garrisonville Road in North Stafford, at 1:35 a.m. Saturday. The burglar broke into a back hallway but was not able to enter the pharmacy, owner Dan Singh told Stafford Local.

An alarm sounded when the burglar broke in notifying the Stafford sheriff's office. Singh said fled the scene without stealing anything.

This is the third time this has happened at the independent business.

> "Police have always arrived within minutes. The burglar seems to know that after he gets in he only has a few minutes before police arrive," Singh told Stafford Local.

2015 Russian Sukhoi Su-24 shootdown

From Wikipedia, the free encyclopedia

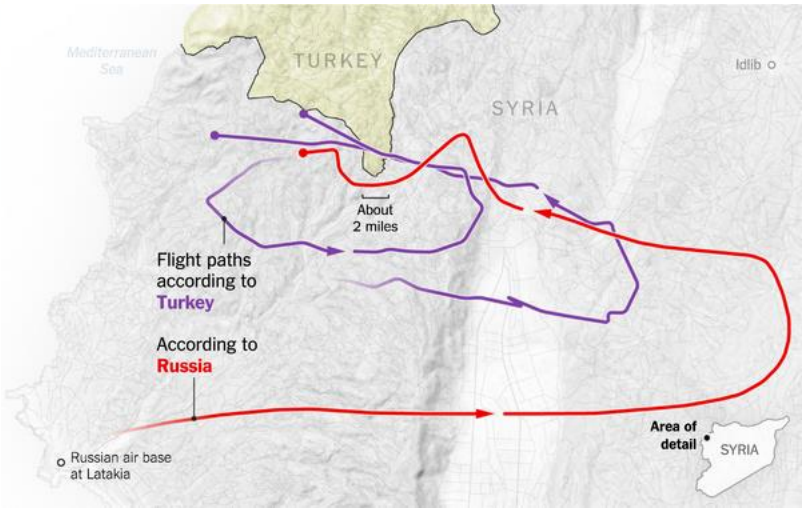
A Turkish Air Force F-16 fighter jet shot down a Russian Sukhoi Su-24M bomber aircraft near the Syria–Turkey border on 24 November 2015.[3][4] According to Turkey, the aircraft—whose nationality was unknown at the time—was fired upon while in Turkish airspace because it violated the border up to a depth of 2.19 kilometres (1.36 miles) for about 17 seconds after being warned to change its heading 10 times over a period of five minutes.[5][6] The Russia Defence Ministry denied the aircraft ever left Syrian airspace, counter-claiming that their satellite data showed that the Sukhoi was about 1,000 metres (1,100 yd) inside Syrian airspace when it was shot down.[7] The US State Department said that the US independently confirmed that the aircraft's flight path violated Turkish territory, and that the Turks gave multiple warnings to the pilot, to which they received no response.[8][9] Russian president Vladimir Putin said that the US knew the flight path of the Russian jet and should have informed Turkey; two US officials said that Russia did not inform the US military of its jet's flight plan.[10]

The Russian pilot and weapon systems officer both ejected from the aircraft. The weapon systems officer was rescued;[1] the pilot was shot and killed by Syrian Turkmen rebel ground fire while descending by parachute.[11] A Russian naval infantryman from the search-and-rescue team launched to retrieve the two airmen was also killed when a rescue helicopter was shot down by the rebels.[11]

2015 Russian Sukhoi Su-24 shootdown

A Russian Sukhoi Su-24M at Khmeimim airbase, similar to that shot down

Shootdown summary	
Date	24 November 2015
Summary	Shootdown by Turkish Air Force F-16 fighter jet
Site	Syria–Turkey border



Ref:
http://potomaclocal.com/2015/12/13/burglar-targets-stafford-pharmacy/

https://en.wikipedia.org/wiki/2015_Russian_Sukhoi_Su-24_shootdown

http://static01.nyt.com/images/2015/11/24/world/middleeast/russia-turkey-jet-shoot-down-maps-1448382166586/russia-turkey-jet-shoot-down-maps-1448382166586-articleLarge-v3.png

GhostNet, March 2009

JR02-2009

Tracking *GhostNet*:

Investigating a *Cyber Espionage* Network

Information Warfare Monitor
March 29, 2009

TheSecDevGroup

http://www.infowar-monitor.net/ghostnet
http://www.tracking-ghost.net

MUNK CENTRE FOR INTERNATIONAL STUDIES AT TRINITY COLLEGE

Internet | Sun Mar 29, 2009 2:53pm EDT

Canadians find vast computer spy net

WASHINGTON

A web-user views the global networking site called Xing in Stockholm, November 20, 2008. Canadian researchers have uncovered a vast electronic spying operation that infiltrated computers and stole documents from government and private offices around the world, including...
REUTERS/BOB STRONG/FILES

Canadian researchers have uncovered a vast electronic spying operation that infiltrated computers and stole documents from government and private offices around the world, including those of the Dalai Lama, The New York Times reported on Saturday.

In a report provided to the newspaper, a team from the Munk Center for International Studies in Toronto said at least 1,295 computers in 103 countries had been breached in less than two years by the spy system, which it dubbed GhostNet.

Embassies, foreign ministries, government offices and the Dalai Lama's Tibetan exile centers in India, Brussels, London and New York were among those infiltrated, said the researchers, who have detected computer espionage in the past.

Ref: http://www.reuters.com/article/us-security-spying-computers-idUSTRE52R2HQ20090329

Shady Rat, August 2011

White Paper

McAfee

Revealed: Operation Shady RAT

Dmitri Alperovitch, VP Threat Research

An investigation of targeted intrusions into 70+ global companies, governments and non-profit organizations during the last 5 years

Wed Aug 3, 2011 7:17pm EDT

Related: TI

"State actor" behind slew of cyber attacks

BOSTON | BY JIM FINKLE

Security experts have discovered an unprecedented series of cyber attacks on the networks of 72 organizations globally, including the United Nations, governments and corporations, over a five-year period.

TRENDII

Security company McAfee, which uncovered the intrusions, said it believed there was one "state actor" behind the attacks but declined to name it, though several other security experts said the evidence points to China.

The long list of victims in the extended campaign include the governments of the United States, Taiwan, India, South Korea, Vietnam and Canada; the Association of Southeast Asian Nations (ASEAN); the International Olympic Committee (IOC); the World Anti-Doping Agency; and an array of companies, from defense contractors to high-tech enterprises.

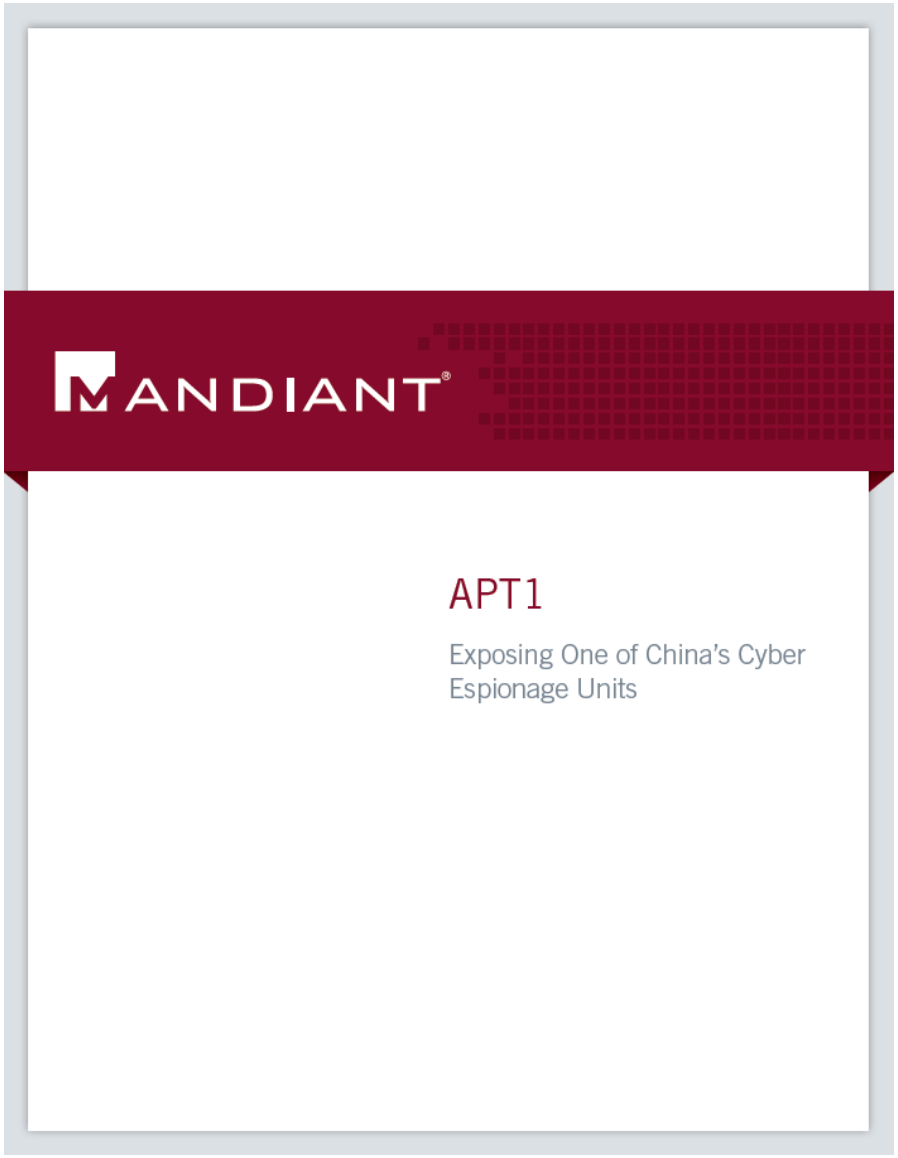
In the case of the United Nations, the hackers broke into the computer system of its secretariat in Geneva in 2008, hid there for nearly two years, and quietly combed through reams of secret data, according to McAfee.

"Even we were surprised by the enormous diversity of the victim organizations and were taken aback by the audacity of the perpetrators," McAfee's vice president of threat research, Dmitri Alperovitch, wrote in a 14-page report released on Wednesday.

"What is happening to all this data ... is still largely an open question. However, if even a fraction of it is used to build better competing products or beat a competitor at a key negotiation (due to having stolen the other team's playbook), the loss represents a massive economic threat."

Ref: http://www.reuters.com/article/us-cyberattacks-idUSTRE7720HU20110803

APT1, February 2013



Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators

February 19, 2013 | by Dan Mcwhorter

Today, The Mandiant® Intelligence Center™ released an unprecedented report exposing APT1's multi-year, enterprise-scale computer espionage campaign. APT1 is one of dozens of threat groups Mandiant tracks around the world and we consider it to be one of the most prolific in terms of the sheer quantity of information it has stolen.

Highlights of the report include:

- Evidence linking APT1 to China's 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (Military Cover Designator 61398).
- A timeline of APT1 economic espionage conducted since 2006 against 141 victims across multiple industries.
- APT1's modus operandi (tools, tactics, procedures) including a compilation of videos showing actual APT1 activity.
- The timeline and details of over 40 APT1 malware families.
- The timeline and details of APT1's extensive attack infrastructure.

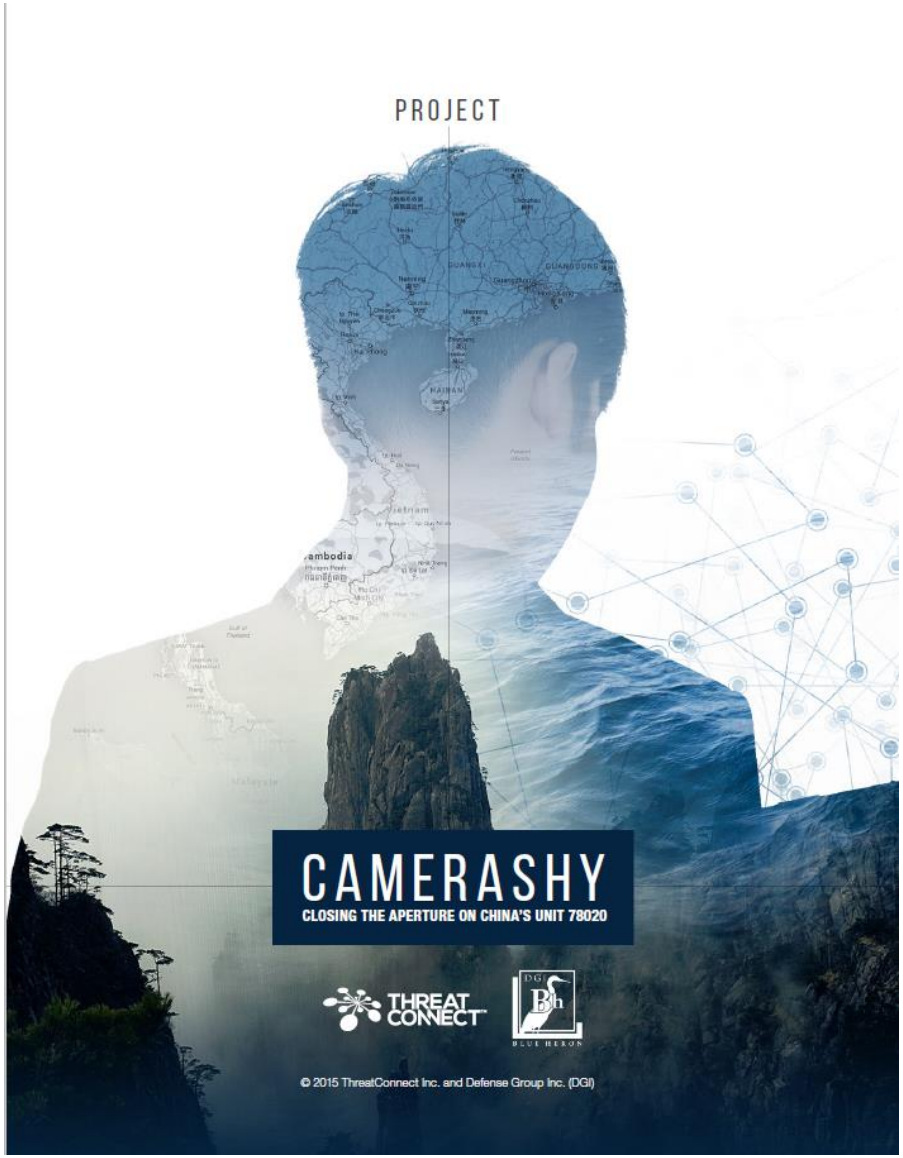
Mandiant is also releasing a digital appendix with more than 3,000 indicators to bolster defenses against APT1 operations. This appendix includes:

- Digital delivery of over 3,000 APT1 indicators, such as domain names, and MD5 hashes of malware.
- Thirteen (13) X.509 encryption certificates used by APT1.
- A set of APT1 Indicators of Compromise (IOCs) and detailed descriptions of over 40 malware families in APT1's arsenal of digital weapons.
- IOCs that can be used in conjunction with Redline™, Mandiant's free host-based investigative tool, or with Mandiant Intelligent Response® (MIR), Mandiant's commercial enterprise investigative tool.

The scale and impact of APT1's operations compelled us to write this report. The decision to publish a significant part of our intelligence about Unit 61398 was a painstaking one. What started as a "what if" discussion about our traditional non-disclosure policy quickly turned into the realization that the positive impact resulting from our decision to expose APT1 outweighed the risk of losing much of our ability to collect intelligence on this particular APT group. It is time to acknowledge the threat is originating from China, and we wanted to do our part to arm and prepare security professionals to combat the threat effectively. The issue of attribution has always been a missing link in the public's understanding of the landscape of APT cyber espionage. Without establishing a solid connection to China, there will always be room for observers to dismiss APT actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns. We hope that this report will lead to increased

Ref: https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html

Camerashy, September 2015



by Michael Mimoso Follow @mike_mimoso September 24, 2015 , 1:37 pm

Chinese president Xi Jinping is supposed to have dinner this evening with U.S. president Barack Obama. Wonder if the name Ge Xing will come up?

Ge Xing is the subject of a joint report published this morning by ThreatConnect and Defense Group Inc., computer and national security service providers respectively. Ge is alleged to be a member of the People's Liberation Army unit 78020, a state-sponsored hacking team whose mission is to collect intelligence from political and military sources to advance China's interests in the South China Sea, a key strategic and economic region in Asia with plenty of ties to the U.S.

The report connects PLA 78020 to the Naikon advanced persistent threat group, a state-sponsored outfit that has followed the APT playbook to the letter to infiltrate and steal sensitive data and intellectual property from military, diplomatic and enterprise targets in a number of Asian countries, as well as the United Nations Development Programme and the Association of Southeast Asian Nations (ASEAN).

Related Posts

Relentless Sofacy APT Attacks Armed With Zero Days, New Backdoors
December 4, 2015 , 7:05 am

China APT Gang Targets Hong Kong Media via Dropbox
December 1, 2015 , 11:37 am

Ref: https://threatpost.com/naikon-apt-group-tied-to-chinas-pla-unit-78020/114798/

Camerashy Doxes PLA 78020 Operative Ge Xing, Resident of Kunming, Yunan province

Figure 18A: QQ Weibo account with username GreenSky27 contained more than 700 posts and photo albums with more than 500 photographs.

Figure 18B: GreenSky27 – both photos posted to QQ Weibo in 2013 (redacted by ThreatConnect).

Figure 21: Image of bicycle for sale by "Mr. Ge" in online forums for Lincang Township (left). Image from GreenSky27's QQ Weibo account, showing another mountain bike located in the same room (right).

Finally, the surname Ge is again connected to the GreenSky27 QQ Weibo account by a 2012 post on Baidu Tieba, in which GreenSky27 announces the birth of his child. The November 21, 2012 post, from Baidu Tieba account "greensky27," states: "A [child], surnamed Ge, born November 20, 2012, at 11:36PM: seeking recommendations for a three-character name."[45]

Confirming the Location: Ge Xing is in Kunming

The advertisements described above place Ge Xing in Kunming. Although his QQ Weibo account lists his physical address as Ireland, numerous images uploaded to this account, including his license plate, geolocated bike routes, and photographs of landmarks in Kunming, place Ge Xing in Kunming.

YUNNAN LICENSE PLATE

The license plate attached to Ge Xing's car, a Volkswagen Golf, indicates a Yunnan Province (云南省) registration. The following photo is representative of several pictures depicting the vehicle and rear plate. The Chinese character on the left end of the plate is "Yun" (云), signifying Yunnan, and the letter A signifies Kunming.

Figure 22: Yunnan license plate on GreenSky27's VW Golf.

45 tieba.baidu.com/p/1928480963?pn=21, accessed July 9, 2015.

Ref: https://www.threatconnect.com/camerashy/

Photos Taken by Ge Xing
Placing Him in the 78020 TRB Building

Parking Lot and a Structure Resembling a Water Tower

Another series of photos sharing a similar vantage point appears to depict a parking lot and several nearby locations within the Kunming TRB compound. These photos appear to have been taken between March and December 2013 from within the central building in the Kunming TRB compound. In Google Earth and on QQ Streetview, there is a structure shaped like a water tower that matches the structure on the right side of Ge Xing's photos.

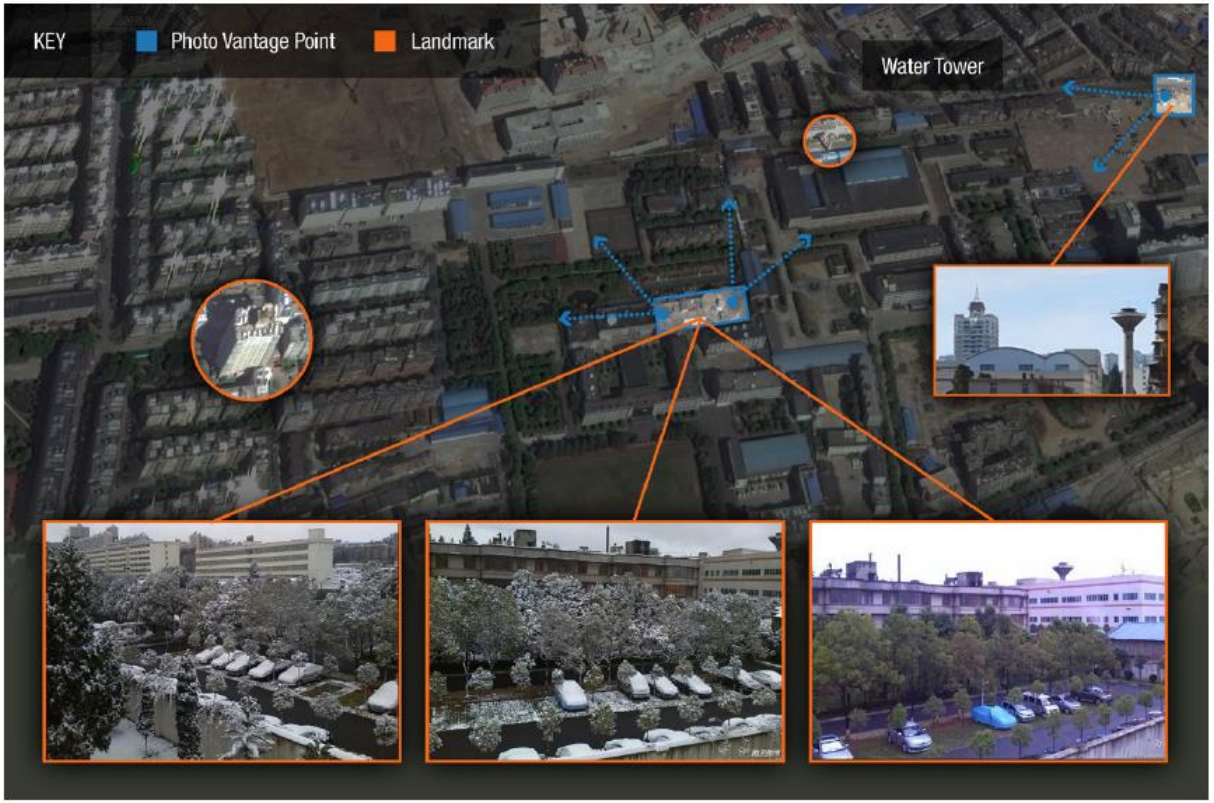


Figure 36: Photos from within Unit 78020 of the parking areas with background landmark of a water tower (bottom three images). QQ Streetview image of landmark of building with distinctive roof ornament and water tower (middle right).

Ref: https://www.threatconnect.com/camerashy/

Photos Taken by Ge Xing Placing Him in the 78020 TRB Building

Courtyard Within the Kunming TRB Compound

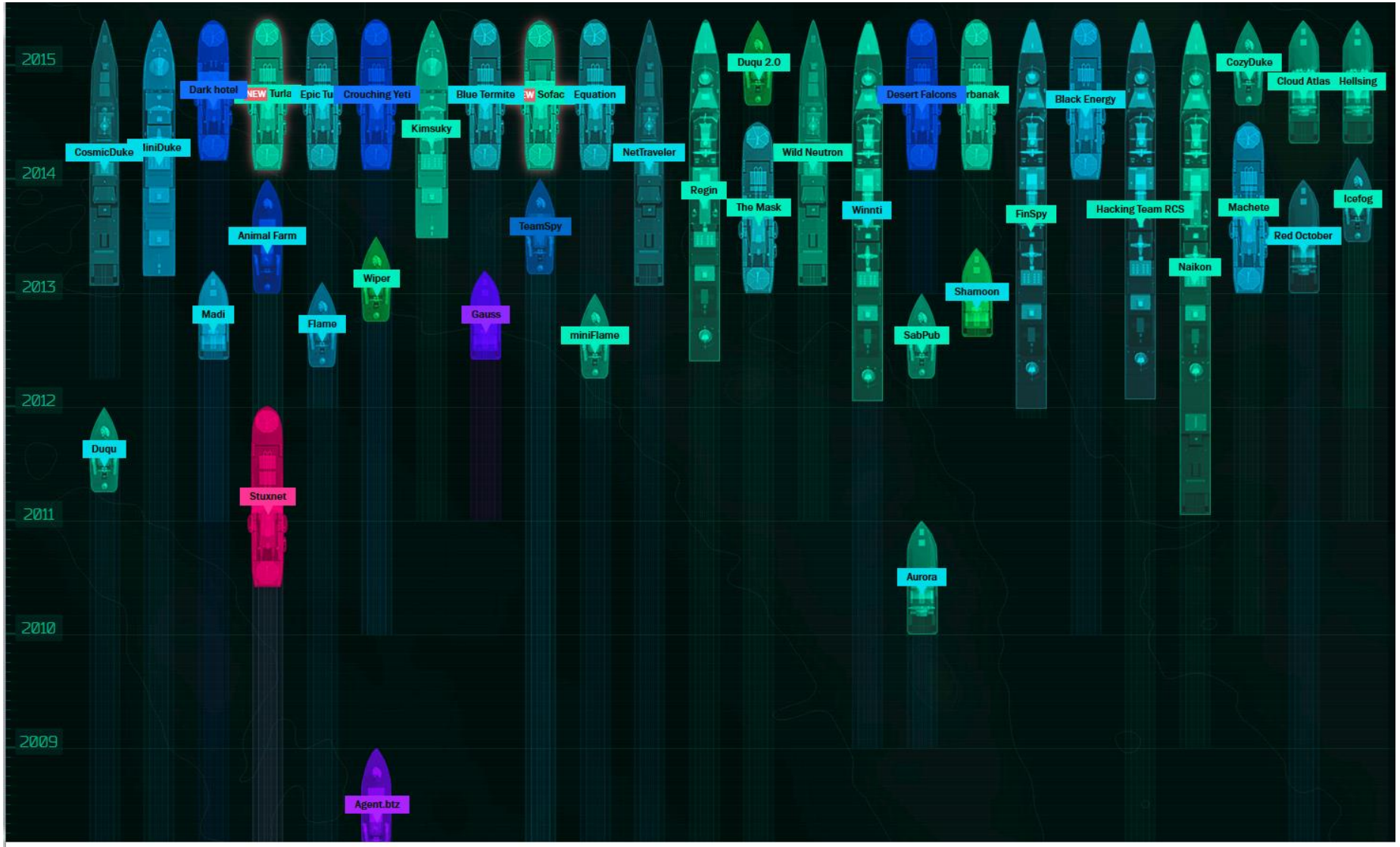
On September 3, 2013, Ge Xing took a photo of a courtyard, the pattern of which matches the two courtyards in the middle of the main building for the Kunming TRB.

Figure 37: Photo from within Unit 78020's main compound courtyard.

In short, the totality of evidence from online Chinese media confirms both GreenSky27's identity as Ge Xing and Ge's affiliation with PLA Unit 78020. Online social media accounts, geolocated trips and photos, and references to a physical address confirm Ge Xing's identity and location in Kunming. Ge's military, academic, and publication background strongly hint at his PLA responsibilities, and his photos at the Kunming TRB's main building itself provide definitive proof of association.

Ref: https://www.threatconnect.com/camerashy/

Kaspersky APT Tracker



Ref: http://apt.securelist.com

New Exposures: China's Qihoo 360 Sky Labs Reveals Possible Vietnamese Hacking Team

"海莲花"APT报告：攻击中国政府海事机构的网络空间威胁

360安全卫士 (/author/360安全卫士) · 2015/05/29 14:40

0x00 OceanLotus概述

2012年4月起至今，某境外黑客组织对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。该组织主要通过鱼叉攻击和水坑攻击等方法，配合多种社会工程学手段进行渗透，向境内特定目标人群传播特种木马程序，秘密控制部分政府人员、外包商和行业专家的电脑系统，窃取系统中相关领域的机密资料。

根据该组织的某些攻击特点，我们将其命名为OceanLotus。

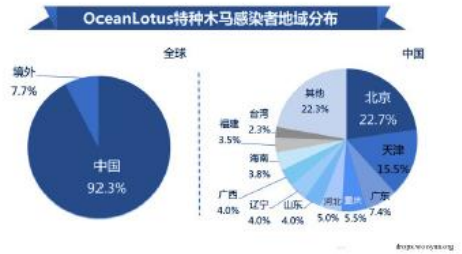
目前已经捕获的与OceanLotus相关的第一个特种木马出现在2012年4月。在此后的3年中，我们又先后捕获了与该组织相关的4种不同形态的特种木马程序样本100余个，这些木马的感染者遍布国内29个省级行政区和境外的36个国家。此外，为了隐蔽行踪，该组织还至少先后在6个国家注册了用于远程控制被感染者的C2（也称C&C，是Command and Control的缩写）服务器域名35个，相关服务器IP地址19个，服务器分布在全球13个以上的不同国家。

从OceanLotus发动攻击的历史来看，以下时间点和重大事件最值得关注：

1. 2012年4月，首次发现与该组织相关的木马。OceanLotus组织的渗透攻击就此开始。但在此后的两年左右时间里，OceanLotus并不活跃。
2. 2014年2月，OceanLotus开始通过鱼叉攻击的方法对我们国内目标发起定向攻击。OceanLotus进入活跃期，并在此后的14个月内对我国多个目标发动了不间断的持续攻击。
3. 2014年5月，OceanLotus对国内某权威海洋研究机构发动大规模鱼叉攻击，并形成了过去14个月中鱼叉攻击的最高峰。
4. 同样是在2014年5月，OceanLotus还对国内某海洋建设机构的官方网站进行了篡改和挂马，形成了第一轮规模较大的水坑攻击。
5. 2014年6月，OceanLotus开始大量向中国渔业资源相关机构团体发鱼叉攻击。
6. 2014年9月，OceanLotus针对于中国海域建设相关行业发起水坑攻击，形成了第二轮大规模水坑攻击。
7. 2014年11月，OceanLotus开始将原有特种木马大规模的更换为一种更具攻击性和隐蔽性的云控木马，并继续对我国境内目标发动攻击。
8. 2015年1月19日，OceanLotus针对中国政府某海事机构网站进行挂马攻击，第三轮大规模水坑攻击形成。
9. 2015年3月至今，OceanLotus针对更多中国政府直属机构发起攻击。

通过对OceanLotus组织数年活动情况的跟踪与取证，我们已经确认了大量的受害者。下图为2014年2月至今，全球每月感染OceanLotus特种木马的电脑数量趋势分布。

从地域分布上看，OceanLotus特种木马的境内感染者占全球感染总量的92.3%。而在境内感染者中，北京地区最多，占22.7%，天津次之，为15.5%。



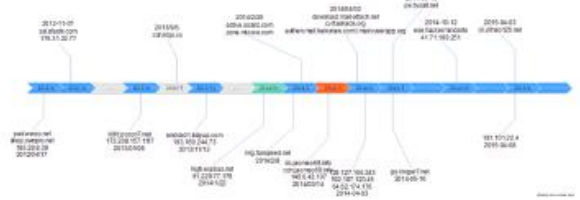
下图为境内OceanLotus特种木马感染者数量地域分布图。

技术分析显示，初期的OceanLotus特种木马技术并不复杂，比较容易发现和查杀。但到了2014年以后，OceanLotus特种木马开始采用包括文件伪装、随机加密和自我销毁等一系列复杂的攻击技术与安全软件进行对抗，查杀和捕捉的难度大大增加。而到了2014年11月以后，OceanLotus特种木马开始转向云控技术，攻击的危险性、不确定性与木马识别查杀的难度都大大增强。

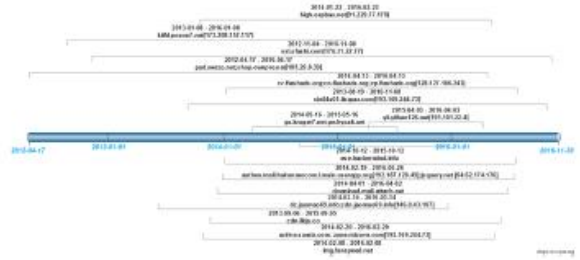
综合来看，OceanLotus组织的攻击周期之长（持续3年以上）、攻击目标之明确、攻击技术之复杂、社工手段之精准，都说明该组织绝非一般的民间黑客组织，而很有可能是具有国外政府支持背景的、高度组织化的、专业化的境外国家级黑客组织。

4. 域名变换

为了隐藏自己的真实身份，OceanLotus组织经常变换下载服务器和C2服务器的域名和IP。统计显示，在过去的3年中，该组织至少使用了C2服务器域名35个，相关服务器IP地址19个。而且大多数域名为了抵抗溯源都开启了Whois域名隐藏，使得分析人员很难知道恶意域名背后的注册者是谁。下图给出了OceanLotus注册各个域名时间点信息。



通过对攻击活动相关域名的统计，我们按注册时间的先后顺序对各个域名做了排序。时间线疏密程度显示该组织在2014年2月至2014年4月申请了大量的新域名。域名的生命周期如下图所示：



这些恶意域名的注册地和服务器也分布在世界各地。从注册地来看，最大的注册地是巴哈马10个，其次是美国4个，尼日利亚3个。从服务器实际所在地来看，美国和乌克兰最多，各5个，其次是瑞典4个，以色列3个。

Ref: http://drops.wooyun.org/papers/6335

New Exposures: China's Qihoo 360 Sky Labs Reveals Possible Vietnamese Hacking Team

OceanLotus: China Hits Back With Its Own Cybersecurity Report

by Adam Segal
June 3, 2015


“海莲花“曝光 蓝翔之冤能否洗白

2015-06-01 17:05:27 来源: 甘肃农民报(兰州)

分享到：

这两天，安全圈最大的事当属360旗下天眼实验室揪出了一朵“恶之花”。一个名为“海莲花”的境外黑客组织攻击中国长达三年，是不是真爱不知道，但如此专一，背后一定有不可告人的秘密。从天眼实验室公布的APT(高级持续性威胁)报告上来看，海莲花的攻击重点是中国政府、科研院所、海事机构、海域建设、航运企业等相关部门。目的也很明确，窃取机密文件。

Ref:
http://blogs.cfr.org/cyber/2015/06/03/oceanlotus-china-fights-back-with-its-own-cybersecurity-report/

http://news.163.com/15/0601/17/AR1Q8SBC00014AEF.html

A rather elaborate, flowery **article** in an unexpected source, Gansu Peasant Daily (甘肃农民报; this could be a reprint from another source, though I have yet to find the original), describes the importance of APT reports to China. The article notes that before OceanLotus, China had never had an APT report that was “up to par.” As a result, U.S. companies, and the United States government, could use the reports to go on the offensive:

> As long as they have an APT attack report they can read off, even if they're playing at being hoodlums, they're doing it rationally and in accord with the law. China has been locked in a closet with grievances it can't speak out against, with no choice but to swallow them down, suffering in silence.

Now, with OceanLotus, China does not have to be so passive. In fact, it can now push back. The article continues:

> From now on, China can pop out this report, confidently face other nations and say: “Look! We've been attacked for three years. You always say that we're conducting attacks. Let's take this outside and talk it out!”

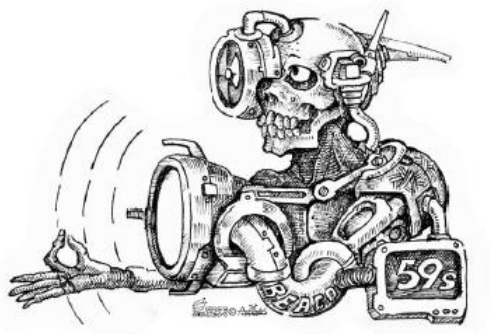
The Chinese foreign ministry wasted no time in using the report. In the June 2 press **conference**, Foreign Ministry Spokesperson Hua Chunying responded to a question about OceanLotus by saying that “If what has been reported is true, it proves once again that China is the victim of hacker attacks.”

New Exposures: China's Antiy Labs Notices Someone Attacking with Cobalt Strike

ANTIY

ANALYSIS ON APT-TO-BE ATTACK THAT FOCUSING ON CHINA'S GOVERNMENT AGENCY

Antiy CERT



First release time: 14:32, May 27, 2015
Updated time of this version: 14:32, May 27, 2015

Author of Cobalt Strike: Raphael Mudge

Raphael Mudge is the founder of Strategic Cyber LLC, a Washington, DC based company that creates software for red teams. He created Armitage for Metasploit, the Sleep programming language, and the IRC client jIRCii. Previously, Raphael worked as a security researcher for the US Air Force, a penetration tester, and he even invented a grammar checker that was sold to Automattic. His work has appeared in Hakin9, USENIX ;login:, Dr. Dobb's Journal, on the cover of the Linux Journal, and the Fox sitcom Breaking In. Raphael regularly speaks on security topics and provides red team support to many cyber defense competitions.

Education background: Syracuse University, Michigan Technological University

Current position: Strategic Cyber LLC , Delaware Air National Guard

Skills: software development, information security, object-oriented design, distributed system, figure interface, computer network design, blog system, social engineering, security research and so on.

Company/Project/Organization	Postion	Time
Strategic cyber LLC	Founder and Principal	January, 2012-now
Delaware Air National Guard	Major	2009-now
Cobalt strike	Principal Investigator	November, 2011- May, 2012
TDI	Senior Security Engineer	August, 2010 – June, 2011
Automattic	Code Wrangler	July, 2009 – August, 2010
Feedback Army, After the Deadline	Founder	July, 2008 –November, 2009
Air Force Research Laboratory	Systems Engineer	April, 2006 – March, 2008
US Air Force	Communications and Information Officer	March, 2004 - March, 2008

Ref: http://www.antiy.net/p/analysis-on-apt-to-be-attack-that-focusing-on-chinas-government-agency/

Risk: Whom to Trust?

Introduction

This document summarizes the open sour
(MH17) on July 17, 2014 in Ukraine. It draws
information to uncover facts about the eve
launcher that downed MH17.

The Buk Missile Launcher

After the downing of MH17 on July 17, a nu
show the movements of a Buk missile laur
confirm the location where each image wa
evidenced when and where the Buk missil
timeline of where the Buk was and when:

- 10:45 am: Departed Donetsk eastb
- 11:00 am – 12:00 pm: Passed Zuhre
- 12:00 pm – 12:45 pm: Entered and t
- 1:00 pm: Entered Snizhne
- 1:30 pm – 2:30 pm: Buk was unloac (southbound)
- 4:20 pm: MH17 shot down

Before the first reports and images of the
communications intercepted by the Ukrair
movements of the Buk missile launcher. In
and references to a location inside Donetsk known as the "Motel."[4] The Motel, located in the east of Donetsk and used by separatist forces as a base, is close to locations described in social media postings by Donetsk locals who reported sightings of a Buk missile launcher being transported through the city. These sightings are also close to the location where two images showing a Buk missile launcher being transported on the back of a red low-loader were taken, later published by Paris Match[3] and Bellingcat.[4]

[1] https://www.youtube.com/watch?v=MVAOTWPmMM4&t=4m16s
[2] https://www.youtube.com/watch?v=MVAOTWPmMM4&t=3m5s
[3] http://www.parismatch.com/Actu/International/EXCLU-MATCH-Un-camion-vole-pour-transporter-le-systeme-lance-missiles-577289
[4] https://www.bellingcat.com/news/uk-and-europe/2015/01/17/new-images-of-the-mh17-buk-missile-launcher-in-ukraine-and-russia/

bellingcat

Eliot Higgins
@EliotHiggins
Follow

.@ruptly films the cluster bombs mounted on Russian jets that Russia denies using in Syria youtube.com/watch?v=RcjJjx…

RETWEETS 315 LIKES 100

2:17 AM - 2 Jan 2016

YouTube

Possible Russian cluster bomb sightings in Syria

Brown Moses
Subscribe 1,319

2,663

Download Add to Share More 17 9

Uploaded on Dec 31, 2015
1 https://www.youtube.com/watch?v=EYnF_...
0:20 to 0:27
2 https://www.youtube.com/watch?v=FDCOt...

SHOW MORE

ALL COMMENTS (27)

Add a public comment...

Top comments

Withnail1969 2 days ago
none of these are cluster bombs.

1 and 2 are old style OFAB 250 freefall general purpose bombs, as opposed to the OFAB 250/270 which are mostly used.

3 and 4 are guided 500 kg bombs.
Read more

Ref: https://twitter.com/EliotHiggins/status/683230619489427457 and https://www.bellingcat.com/wp-content/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf and https://www.youtube.com/watch?v=RcjJjxFtAC0

Risk: Going Too Far by Attacking Poison Ivy Servers...

Public document

APT1: technical backstage

malware analysis

Ref:
https://malware.lu/articles/2013/04/08/apt1-technical-backstage.html

General information		
Sequence number	002	
Version	1.0	Ref: https://malware.lu/articles/2013/04/08/apt1-technical-backstage.html
State	Final	
Approved by	Paul Rascagnères	
Approval date	27/03/2013	
Classification	Public	

1.1 Context

The company Mandiant published in February 2013 a report about an Advance Persistent Threat (APT) called APT1. The report can be freely downloaded here: http://intelreport.mandiant.com/.

Inspired by this article, we have decided to perform our own technical analysis of this case. In the report, Mandiant explains that the attackers were using a well-known Remote Administration Tool (RAT) called Poison Ivy and that they were located in China. We based our investigation based on those two facts only.

1.2 Objectives

The objective of the mission was to understand how these attackers work. Our purpose was to identify their infrastructures, their methodologies and also the tools they used. We are convinced that in order to protect our infrastructures against this kind of attacks, we need to analyse, learn and understand the way attackers work.

1.3 Authors

This report has been created by Malware.lu CERT, the first private Computer Security Incident Response Team (CSIRT) located in Luxembourg and itrust consulting S.A.R.L, a Luxembourg based company specialising in formation system security.

2.2 IP ranges

After removing false positives, we identified 6 IP ranges where Poison Ivy Command & Control servers were running:

- 113.10.246.0 - 113.10.246.255: managed by NWT Broadband Service
- 202.65.220.0 - 202.65.220.255: managed by Pacific Scene
- 202.67.215.0 - 202.67.215.255: managed by HKNet Company
- 210.3.0.0 - 210.3.127.255: managed by Hutchison Global Communications
- 219.76.239.216 - 219.76.239.223: managed by WINCOME CROWN LIMITED
- 70.39.64.0 – 70.39.127.255: managed by Sharktech

3.4 Exploitation

With the information we previously described, we were able to get access to the attackers servers.

```
msf  exploit(poisonivy_bof_v2) > show options

Module options (exploit/windows/misc/poisonivy_bof_v2):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   Password    pswpsw           yes       Client password
   RANDHEADER  false            yes       Send random bytes as the header
   RHOST       X.X.X.X          yes       The target address
   RPORT       80               yes       The target port
```

...But Finding Interesting Data and Infrastructure Anyway?

4.3 Targets

The attackers seem to use a dedicated proxy and Poison Ivy server combination for each target. When a target discovers the IP address of a proxy, this address is reassigned to another target. That's why it is **primordial to share the C&C servers IPs with our partners**. The targets were private and public companies, political institutions, activists, associations or reporters.

On the Poison Ivy server, a directory is created for every target. Within this directory, a directory for each infected machine was created. The naming convention for those directories is HOSTNAME^USERNAME. Here is an example:

```
E:\companyABCD\alien^rootbsd\
```

In those directories files are not sorted in any specific manner. The documents types are:

- .PPT
- .XLS
- .DOC
- .PDF
- .JPG

Among those documents, we found:

- Network diagrams;
- Internal IP/user/password combination (local administrator, domain administrator, root, web, webcam…);
- Map of the building with digital code to open doors;
- Security incident listings;
- Security policies;
- …

The sensitive documents were password protected. The passwords pattern is [a-z]{3,4}[0-9]{3,4}, so it was easy to brute force them in reasonable time. Here is an example of a network diagram.

Number	Net block	Registered Owner
445	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
217	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
114	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
12	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
1	114.80.0.0 - 114.95.255.255	China Telecom Shanghai Network
1	101.80.0.0 - 101.95.255.255	China Telecom Shanghai Network
27	Other (non-Shanghai) Chinese IPs	

Majority of APT1 China-based infrastructure located in Shanghai...

Ref:
https://intelreport.mandiant.com

2.2 IP ranges

After removing false positives, we identified 6 IP ranges where Poison Ivy Command & Control servers were running:

- 113.10.246.0 - 113.10.246.255: managed by NWT Broadband Service
- 202.65.220.0 - 202.65.220.255: managed by Pacific Scene
- 202.67.215.0 - 202.67.215.255: managed by HKNet Company
- 210.3.0.0 - 210.3.127.255: managed by Hutchison Global Communications
- 219.76.239.216 - 219.76.239.223: managed by WINCOME CROWN LIMITED
- 70.39.64.0 – 70.39.127.255: managed by Sharktech

But Malware.lu decided to scan and exploit IP blocks in Hong Kong?

Ref:
https://malware.lu/articles/2013/04/08/apt1-technical-backstage.html

Risk: Going Too Far by Pursuing Defense Personnel

IAF official arrested after leaking secrets to ISI honey-trapper pretending to be 'UK-based woman'

- **Ranjith KK believed he was talking to a female media executive**
- **But 'Damini McNaught' was actually a honey-trap set up by Pakistani spies**
- **Ranjith has been booked under the Official Secrets Act**

By SHASHANK SHEKHAR

PUBLISHED: 17:08 EST, 29 December 2015 | **UPDATED:** 17:08 EST, 29 December 2015

Share

View comments

An Indian Air Force official allegedly passed on secret information to Pakistani spy agency the ISI after landing into a honey-trap.

All it took was a fake Facebook profile for a 'UK-based woman'.

Sacked Indian Air Force (IAF) official Ranjith KK was on Monday arrested by Delhi Police's Crime Branch from Punjab's Bathinda city. Police sources revealed that the officer was honey-trapped by ISI agents, who created a fake profile for a woman by the name of Damini McNaught, who was claimed to be an executive at a UK-based media firm.

Ranjith KK (centre) has been sent to four-day police custody after unwittingly passing on the information

"The woman befriended the airman and started extracting information about the air force. The officer never knew that he was passing on information to the Pakistani agency. She started taking details from him online on the pretext of an article on the IAF. Ranjith shared information on a number of fighter jets and also details of each and every building at his air force station," a senior police officer said.

For an article McNaught claimed that she required Air Force-related information for an article she was writing for their news magazine.

"Ranjith shared Air Force-related information, mostly pertaining to deployment, recent exercises, movements and status of aircraft. He was being used to identify each building inside the Bathinda air force camp. After seeing Google map, she was asking him about the nature of the building. He helped them identify the air traffic controller building, the parking place of jet planes, connecting runway and bunker for the aircraft," an officer investigating the case told Mail Today, adding that Ranjith was unintentionally passing on information to Pakistan.

The officer claims that Ranjith was passing information in exchange for money. Money amounting to Rs 30,000- 50,000 was transferred twice into his bank account.

Indian hackers are monitoring current and retired defence personnel to stop leaks to international spies

By SHASHANK SHEKHAR

PUBLISHED: 18:30 EST, 31 December 2015 | **UPDATED:** 18:29 EST, 31 December 2015

Share

View comments

A group of Indian hackers is gearing up to keep a close eye on serving and retired defence personnel to ensure they are not passing information to international spies on the virtual world.

The move by the hacking community is to ensure that no information is being leaked via social networking websites which can be used against the nation.

The step was taken after reports of defence personnel's involvement in the ISI spy racket surfaced.

The Crime Branch of Delhi Police on Monday arrested IAF airman Ranjith KK, who was honey trapped by Pakistan's ISI agency via a fake profile on Facebook.

Experts claim spies from countries like Pakistan, the US and China are interested in gathering info from India. (File picture)

He had been talking to "pretty woman" Damini McNaught for the last several months on Facebook and was passing sensitive details related to the Air Force.

Recently, security agencies arrested serving and retired defence personnel from various locations who were leaking information to Pakistani security agency the ISI.

"We will follow the modus operandi used by international agents. We will track Indian officers and will try to get information from them. The moment they pass any information, we will alert the security agency giving proof against them," said a hacker who claims to be a part of ethical hacking community Anonymous-India.

Ref:
http://www.dailymail.co.uk/indiahome/indianews/article-3380646/Indian-hackers-monitoring-current-retired-defence-personnel-stop-leaks-international-spies.html

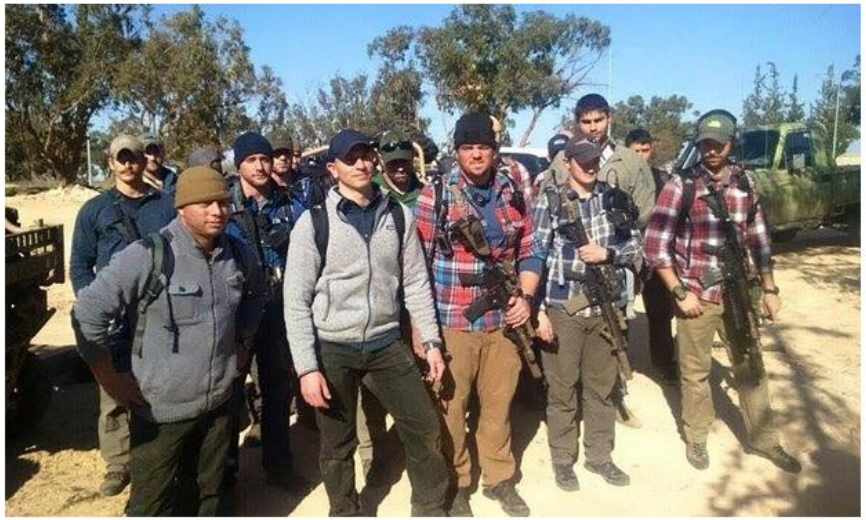
and

http://www.dailymail.co.uk/indiahome/indianews/article-3377996/IAF-official-arrested-leaking-secrets-ISI-honey-trapper-pretending-UK-based-woman.html

Risk: Damaging National Security?

Secret US mission in Libya revealed after air force posted pictures

Facebook post, accompanied by four pictures, said 20 armed soldiers arrived wearing bulletproof jackets



Photographs showed three Americans armed with assault rifles. Photograph: Libyan Air Force/Facebook

A secret US commando mission to Libya has been revealed after photographs of a special forces unit were posted on the Facebook page of the country's air force.

Libya's air force said 20 US soldiers arrived at Libya's Wattiya airbase on Monday, but left soon after local commanders asked them to go because they had no permission to be at the base. It was unclear if another branch of the Libyan military had authorized the mission.

Pentagon sources confirmed to US media that the special forces unit was part of a mission sent this week, but it was unclear if the soldiers had left the country.

Ref: http://www.theguardian.com/us-news/2015/dec/17/secret-us-mission-in-libya-revealed-after-air-force-posted-pictures and https://www.facebook.com/libyan.air.forces/photos/pb.427396087290661.-2207520000.1451937846./1071557676207829/?type=3&permPage=1

Bonus: Instant Analysis

Babak Taghvaee @BabakTaghvaee · 17 Dec 2015
A C-146A of #USAF's 524th SOS with 11-3097 s/n and N307EF civ
carried US Commandos to Libya on 14th Dec.

24 15

Oryx
@oryxspioenkop
Follow

@BabakTaghvaee So to familiarize with Islamic State held parts of Libya near Sirte, Delta Force goes to Tripoli?

RETWEETS 2 LIKE 1

5:12 AM - 17 Dec 2015

Babak Taghvaee @BabakTaghvaee · 17 Dec 2015
@oryxspioenkop It appears that the Watiya AB is more important for the Americans, and they will probably want to protect it as a hub.
1

Babak Taghvaee @BabakTaghvaee · 17 Dec 2015
@oryxspioenkop Also al-Watiya is under control of Internationally recognized Tobruk GOV.

Babak Taghvaee @BabakTaghvaee · 17 Dec 2015
@oryxspioenkop I mean not only ISIS, rather Fajr al-Libya and others as well.

Alex M. @Alex_de_M · 17 Dec 2015
.@oryxspioenkop @BabakTaghvaee They might be poking around the Libya-Tunisia border area: realites.com.tn/2015/12/des-ma…
2 2
View summary

Ref: https://twitter.com/oryxspioenkop/status/677476361880133632?replies_view=true&cursor=AMCUmNbhZgk

Risk: Personal Risks to Security Researchers

Cybersecurity Researchers Are Hunted from All Sides

Written by **ANDRADA FISCUTEAN**

December 14, 2015 // 09:00 AM EST

Cybersecurity researcher Peter Kruse, founder of CSIS Security Group in Denmark, thought his mother was calling. Her number appeared on his phone, but when he answered, it wasn't her. Instead, a male voice told him to stop what he was doing as a computer expert.

"They checked my family members," he said, referring to his anonymous tormenters. "They did their homework."

Security researcher Costin Raiu at Kaspersky Lab in Romania has a similar story. While he was analyzing Stuxnet, a worm written by the US and Israel and considered to be the first cyber weapon, someone broke into his house.

The intruder left behind a decision cube—a rubber die inscribed with conclusions like "yes," "no," "maybe"—on his living room table with the message "take a break" facing up.

These stories of being threatened are common throughout the tight-knit community of high-profile cybersecurity researchers, but few are willing to share them openly.

"If you are engaged in tracking cybercriminals, in research, you have to be really careful about your surroundings, your family, the people around you," said Righard Zwienenberg, ESET security expert. "People doing this kind of research take the risk knowingly and willingly."

Enemies on all sides

While this secretive lifestyle might be alluring to some, most cybersecurity researchers are, by nature, geeks. Computer science taught in high-school and at university level did not prepare them for what can only be described as spy games.

THE ETHICS AND PERILS OF APT RESEARCH: AN UNEXPECTED TRANSITION INTO INTELLIGENCE BROKERAGE

Juan Andrés Guerrero-Saade
Kaspersky Lab, USA

Email juan.guerrero@kaspersky.com

ABSTRACT

The top tier of the information security industry has undergone a tectonic shift. Information security researchers are increasingly involved in investigating state-sponsored or geopolitically significant threats. As a result, the affable and community-friendly information security researcher has become the misunderstood and often imperilled intelligence broker. In many ways, researchers have not come to accept this reality, nor have they prepared to act out their new role. Similarly, our industry has yet to gain insights into the complicated playing field of geopolitical intrigue it has set foot into, and as such has fallen into an identity crisis.

Both individual researchers and top-tier infosec firms face drastic changes in embodying their new role as intelligence brokers. Necessary areas of improvement beyond dispute include the enhancement of geopolitical analysis skills and analytical frameworks, coordinated operational security, and strategic decision-making based on a political calculus befitting heightened stakes and disproportionately powerful players. As this new playing field comes into clear view, so will the perils and ethical conundrums that are its permanent features. In the face of investigations with geopolitical weight and consequences, whose final attributions entail unmasking nation-state operations, even the most capable security researcher among us will need drastic preparations, not only to excel but to survive.

INTRODUCTION – RE-SITUATING OUR CONCEPTUAL COORDINATES

In recent years, the information security industry has undergone a tectonic shift as it has embraced 'cyberespionage' research. Research reports on advanced persistent threats (APTs) and targeted attacks (TAs) have become a commonplace offering for high-end outfits and security startups alike, both fighting for the headlines that accompany 'nation-state attacks'. Though the flashy newcomers often lack the visibility or expertise to properly analyse an APT campaign, the top-tier infosec companies have come to pin their legitimacy on intelligence reports. Despite the analytical strength and scrutiny poured into these, the object of study is largely misunderstood.

The terms 'APT', 'targeted attack', 'nation-state sponsored', and even 'cyberespionage' are inaccurate and misrepresent the object of study, which is to say an espionage operation partially carried out with the use of malware. The execution of this complex task is largely determined by a cross-section between the requirements and resources of the attacker, the particular features of the victim systems, and the dynamic and opportunities between the two. The breadth of interactions that arise therein lend themselves to persistent attacks that are not advanced [1], advanced attacks that are not persistent[1], widely distributed attacks intended for a specific target[2], and targeted attacks with the intention of reaching a wider audience[3]. APT is the generic moniker applied to all of these cases for the sake of convenience and easy marketability, at the expense of accuracy and greater understanding.

Similarly, inexperienced political analysts tilted towards the myopic bias of an intended market audience are wont to botch an investigation already ripe with potential for both misinterpretation and intentional deception on the part of the attacker[4]. Malware is classified as 'nation-state sponsored' regardless of its sophistication based entirely on the stature of its targets and the nature of the data pursued within infected systems. That is to say: 'who, if not the government, is interested in political documents, military dossiers, or industrial control systems?'. One outlier is a subset of attack groups whose interest in political and military secrets is prospectively monetary: with the intention to sell pilfered data to interested parties who may include government institutions but also political opposition, private consulting and political analysts, government contractors, adversarial nation-states, as well as corporations, utilities providers, financial speculators, and a diverse array of institutions whose interests overlap due to governmental regulation and intervention. Further focus on the malware's deployment onto specific systems or its design for stealing specific document types or specific strings may strengthen our conviction that the attackers are after a specific type of data but it gets us no closer to understanding who the final recipient of the pilfered data may be. This goes to say that there exists enough ambiguity to disqualify the term 'nation-space sponsored malware' as vague, if not purposefully inaccurate.

The purpose of this extensive disambiguation is to get at the root of the inadequacy of the broader category of 'cyberespionage' at the level of genuine nation-state attacks. When discussing the operations of a professional institution whose primary activity is intelligence gathering and production, cyberespionage as colloquially defined by the infosec community is largely meaningless. 'Cyber'-capabilities for data gathering are an evolution of the adoption of technological sleight-of-hand that intelligence agencies have spear-headed in order to run uncompromised agent networks as well as more efficiently generate and exfiltrate data. To define espionage by its material means may be momentarily useful insofar as it speaks to attacker capabilities and specific features of the data gathered but to subsequently allow this narrow lens to define the operation as a whole is a mistake. Analogously, it is partially useful to discuss the benefits of concealed microphones in espionage operations but to understand espionage operations through the practice of

[1] With malware residing in memory and leaving minimal footprint on disk, as in the case of Duqu 2.0 [2].
[2] Examples include Darkhotel components [3] and Animal Farm's Nbot [4] intended for DDoS.
[3] Regin's use of legitimate institutions as domestic network proxies [5] or Duqu's utilitarian targeting for digital certificates [6].
[4] Common examples of attributory data manipulation centre around language strings and timestamp manipulation. An example of the former is MiniDuke's attempt to hide Russian-speaking developers with consistent use of English [7] or extensive use of 'red herrings' by CloudAtlas/Inception Framework [8].

Refs: http://motherboard.vice.com/read/cybersecurity-researchers-are-hunted-from-all-sides and http://media.kaspersky.com/pdf/Guerrero-Saade-VB2015.pdf

Thank you

- The Practice of Network Security Monitoring
  - Published July 2013
  - www.nostarch.com/nsm
  - 30% off with code **NSM101**
- Contact
  - @taosecurity
  - taosecurity@gmail.com
  - taosecurity.blogspot.com
  - www.taosecurity.com/research.html