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
Information Warfare Against Serbian Radio Television, 1 October 1997

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

Ref: http://www.iwar.org.uk/iwar/resources/airchronicles/tulak.htm
Watching Vessels Pass through Bosphorus

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Number</th>
<th>Name</th>
<th>Direction</th>
<th>Nationality</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.9.2015</td>
<td>KIL-158</td>
<td>Southbound</td>
<td>Russia</td>
<td></td>
</tr>
<tr>
<td>27.9.2015</td>
<td>152</td>
<td>Nikolay Fitchenkov</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>26.9.2015</td>
<td>150</td>
<td>Saratov</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>25.9.2015</td>
<td>121</td>
<td>Moskva</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>24.9.2015</td>
<td>001</td>
<td>Ladny</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>24.9.2015</td>
<td>952</td>
<td>R-109</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>24.9.2015</td>
<td>31</td>
<td>Alexander Otrakovski</td>
<td>Northbound</td>
<td>Russia</td>
</tr>
<tr>
<td>22.9.2015</td>
<td>151</td>
<td>Azov</td>
<td>Northbound</td>
<td>Russia</td>
</tr>
<tr>
<td>22.9.2015</td>
<td>150</td>
<td>Tseytzer Kunnikov</td>
<td>Northbound</td>
<td>Russia</td>
</tr>
<tr>
<td>21.9.2015</td>
<td>142</td>
<td>Novocharakissi</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>20.9.2015</td>
<td>Donuzliv</td>
<td>Southbound</td>
<td>Russia</td>
<td></td>
</tr>
<tr>
<td>19.9.2015</td>
<td>810</td>
<td>Smolny</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>19.9.2015</td>
<td>KIL-158</td>
<td>Northbound</td>
<td>Russia</td>
<td></td>
</tr>
<tr>
<td>17.9.2015</td>
<td>150</td>
<td>Saratov</td>
<td>Northbound</td>
<td>Russia</td>
</tr>
<tr>
<td>17.9.2015</td>
<td>Saymy</td>
<td>Northbound</td>
<td>Russia</td>
<td></td>
</tr>
<tr>
<td>15.9.2015</td>
<td>Novorossiysk</td>
<td>Northbound</td>
<td>Russia</td>
<td></td>
</tr>
<tr>
<td>15.9.2015</td>
<td>031</td>
<td>Alexander Otrakovski</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>14.9.2015</td>
<td>151</td>
<td>Azov</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>14.9.2015</td>
<td>158</td>
<td>Tseytzer Kunnikov</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>13.9.2015</td>
<td>USS Donald Cook</td>
<td>Southbound</td>
<td>USA</td>
<td></td>
</tr>
<tr>
<td>10.9.2015</td>
<td>152</td>
<td>Nikolay Fitchenkov</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>9.9.2015</td>
<td>KIL-158</td>
<td>Southbound</td>
<td>Russia</td>
<td></td>
</tr>
<tr>
<td>7.9.2015</td>
<td>160</td>
<td>Saratov</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>4.9.2015</td>
<td>210</td>
<td>Smolny</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>3.9.2015</td>
<td>120</td>
<td>Kuravev</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
<tr>
<td>3.9.2015</td>
<td>142</td>
<td>Novocharakissi</td>
<td>Southbound</td>
<td>Russia</td>
</tr>
</tbody>
</table>

Ref: http://turkishnavy.net/2015/10/01/foreign-warship-on-bosphorus-2015-part-43/
Bosphorus?
Bosphorus!
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
Subi Reef
This reef has changed dramatically in recent months. The southern, western, and northern edges of the reef have been reclaimed and an access channel to the inner harbor cut out. Dredgers continued to operate here in June. Two cement plants are being built along the western bank.

38 North Project Tracking North Korean Economic Activity via Satellite Imagery

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

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

(March 12, 2015; Google Earth)

(September 15, 2013; Google Earth)

(March 2, 2015; Google Earth)

(September 6, 2015; Google Earth)

38 North Project Identifies New North Korean Submarine

--- The North Korean Navy Acquires a New Submarine

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 900-1,300 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.

Ref: http://38north.org/2014/10/jbermudez101914/
Reports on Russian Air Strikes in Syria

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 Jund al-Aqsa artillery battalion in the northeastern countryside of Dara’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 strike 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, reports 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.

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

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 Taghvaie reports (as cited by The Aviationist) that Russian Tu-95MS Bear, Tu-160 Blackjack, and Tu-22M Backfire bombers have flown a southwestern 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 Najihe Air Base in the northwestern province of Hamadan, 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:
Crowdsourcing Russian Reports of Airstrikes in Syria

Verifying Russian airstrikes in Syria with Silk, two months on

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

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

Ref: https://russia-strikes-syria.silk.co/
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.
GWU Report on ISIS in America

THE ISIS DEN IN AMERICA

The role of social media in recent developments in the jihadist scene is central, but in some cases it is matched or even exceeded by important real-world dynamics. These sympathizers did not begin their radicalization trajectories alone in front of a computer screen, but rather via face-to-face interactions through preexisting social contacts who already embraced jihadist ideology. Over time, these individuals tend to form a cluster of like-minded individuals whose internal dynamics reinforce the beliefs of its members.

Read the full report: ISIS IN AMERICA FROM RETWEETS TO RAQQA

KEY INDIVIDUAL
Abdullah Ramo Paza, a naturalized U.S. citizen from Bosnia

BACKGROUND
A veteran of the Bosnian civil war, Paza came to America in the 1990s. After his marriage and business unraveled, he developed an interest in a literalist interpretation of Islam. In 2013, he left for Syria, where he commanded a Balkan-dominated ISIS battalion.

CLUSTER FORMATION
Paza was supported by a group of Bosnian Americans, including a handful who hailed from the same Bosnian town. The group purchased supplies for his battalion and raised money for Paza and the families of other ISIS fighters from the Balkans. Authorities dismantled the group in February 2015, arresting six individuals on terrorism-related charges. Paza was reported killed while fighting in Kobane.

INSIDE THE ISIS U.S. ECHO CHAMBER

KEY INDIVIDUAL
Abdi Nur, a Somali American who joined ISIS in 2014 and then offered fake passports and contact information to his friends back in Minnesota

BACKGROUND
From 2007–2009, nearly two dozen individuals, mostly ethnic Somali, left the U.S. to join the terrorist group al-Shabaab.

CLUSTER FORMATION
In 2014, a number of Somali Americans shifted their focus from Somalia to Syria. Since then, at least 15 individuals have joined or tried to join ISIS on the ground, relying on the established network of al-Shabaab supporters. Many grew up in the same community, attended the same schools, and worshiped at the same mosque. Several had family or friends connected to al-Shabaab.

KEY INDIVIDUAL
Nader Saadeh, a New Jersey resident of Jordanian/Palestinian descent

BACKGROUND
In 2012, then-teenage Saadeh shared his jihadist sympathies with Munther Omar Saleh, a like-minded teenager from Queens. Two years later, he involved his older brother Alan Saadeh and Samuel Topaz, a convert to Islam of mixed Jewish/Dominican descent from Fort Lee, N.J. Saleh soon incorporated Staten Island’s Fared Muruni. The five discussed and shared ISIS propaganda both online and off.

CLUSTER FORMATION

ARREST
By the spring of 2015, the group had cemented their plans to join ISIS, unaware that they had been under FBI surveillance for months. Nader successfully traveled to Antrim but was arrested by Jordanian authorities. In the wake of his capture, the FBI arrested the cluster’s four remaining members in the New York area.

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 Esteale, Harleen Gambhir, Katie Menoche
November 17, 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 SVETIs. 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 Lesbos. 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 divisiveness 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:
China Laser and Rail Gun Development Thread Shows Expertise and Collaboration

Physical World Attribution: “Little Green Men”

Richard Bejtlich
@taosecurity

Nice work @dimagnayCNN reporting from #Ukraine #Crimea, asks unflagged soldier where he's from, answer: "Russia."

Little green men (2014 Crimean crisis)

From Wikipedia, the free encyclopedia

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

Little green men (Russian: зелёные человеки, Ukrainian: зелені чоловічки), in Russia Polite People (Russian: вежливые люди, Ukrainian: вежливі люди), 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, 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.

Ref: https://en.wikipedia.org/wiki/Little_green_men_%282014_Crimean_crisis%29
Atlantic Council Report on Russia vs 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,” acting as separatist soldiers with additional manpower and Russian equipment. In addition to Ilya Damayev, two more soldiers, Anton Tumanov and Leonid Kichatkin, profiled in this report represent the troubling 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 arrived there on August 13, 2014, in Slovyansk, 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 Komsomolskaya, 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 Komsomolskaya? 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. “I told him the army wouldn’t be sent to Ukraine. He said, “I need money. I’m not going to be a waste. I’m going to a job. There is no other job anywhere.”

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

Training for Combat

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

Deployment to and Death in Slovyansk

Anton Tumanov and his fellow unit member Robert Artyunyan documented their arrival in Slovyansk on August 13—the same place where, twenty-seven days earlier, the SU-155 system that likely shot down MH17 was spotted hours before the crash.

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

I was in the BTR. The hatches were open, and as a result—[it suffered] a concussion and minor loss of hearing. Robert and I were about two steps from the BTR (that I was in). They did not manage to get away. Robert died on the spot. They gave medical help to Anton. He died on the operating table...Robert, having returned home to the Krasnodar Krai to recover from his injury.

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

Soldier Profile 3. Leonid Kichatkin

Russian 74th 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, Olga, and children in Pochelovo, where he was stationed for his military service. In late July 2014, Pochelovo was under attack, and he spoke to his wife at the end of that week.

Maps showing the average trajectory of craters measured at the Anvrosiivka 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.

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. It was suspected that the origin of this attack was the territory of Russia.

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.


China’s ‘Little Blue Men’ Take Navy’s Place in Disputes

By Christopher P. Cavas

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

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”


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

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 fied 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

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. 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. 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. 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. 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 of its jet’s flight plan.

The Russian pilot and weapon systems officer both ejected from the aircraft. The weapon systems officer was rescued. The pilot was shot and killed by Syrian Turkmen rebel ground fire while descending by parachute. 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.

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

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

February 19, 2013 | by Dan Moir

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 61396).
- 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 61396 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
Camerashy, September 2015

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).

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

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.

![Image of courtyard in the 78020 TRB Building]

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

Ref: http://drops.wooyun.org/papers/6335
New Exposures: China’s Qihoo 360 Sky Labs Reveals Possible Vietnamese Hacking Team

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

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 JPC client JPCiun. 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 Automatic. His work has appeared in Hak5, USENIX, Linux Journal, Dr. Dobbs Journal, on the cover of the Linux Journal, and the Fox squirrel Breaking In. Raphael regularly speaks on security topics and provides red team support to many cyber defense competitions.

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.

<table>
<thead>
<tr>
<th>Company/Project/Organization</th>
<th>Position</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Cyber LLC</td>
<td>Founder and Principal</td>
<td>January, 2012-now</td>
</tr>
<tr>
<td>Delaware Air National Guard</td>
<td>Major</td>
<td>2009-now</td>
</tr>
<tr>
<td>Cobalt Strike</td>
<td>Principal Investigator</td>
<td>November, 2011 - May, 2012</td>
</tr>
<tr>
<td>TDI</td>
<td>Senior Security Engineer</td>
<td>August, 2010 - June, 2011</td>
</tr>
<tr>
<td>Feedback Army, After the Deadline</td>
<td>Founder</td>
<td>July, 2008 - November, 2009</td>
</tr>
</tbody>
</table>

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 source (MH17) on July 17, 2014 in Ukraine. It draws information to uncover facts about the event, launcher that destroyed MH17.

The Buk Missile Launcher

After the downing of MH17 on July 17, a new video showing the movements of a Buk missile launch confirmed the location where each image was evidenced when and where the Buk missile timeline of where the Buk was and when:

- 10:45 am: Departed Donetsk east
- 11:30 am: 12:00 pm: Passed Zmiev
- 12:00 pm - 12:45 pm: Entred into and 1
- 1:00 pm - 1:45 pm: Entered Svitlana
- 1:30 pm - 2:30 pm: Buk was unlocked (southbound)
- 4:20 pm: MH17 shot down

Before the first reports and images of the Buk's movements intercepted by the Ukrainian authorities, movements of the Buk missile launchers, in and references to a location inside Donetsk known as the “market”, 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 truck-wagon were taken, later published by Paris Match and Bellingcat.

1.1 Context


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
- 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 Shartech

3.4 Exploitation

With the information we previously described, we were able to get access to the attacker's servers.

```
msf exploit(poisonivy_bof_v2) > show options
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD</td>
<td>pspsw</td>
<td>yes</td>
<td>Client password</td>
</tr>
<tr>
<td>RANDHEADER</td>
<td>false</td>
<td>yes</td>
<td>Send random bytes as the header</td>
</tr>
<tr>
<td>RHOST</td>
<td>xxx.xxx.xxx</td>
<td>yes</td>
<td>The target address</td>
</tr>
<tr>
<td>REPORT</td>
<td>80</td>
<td>yes</td>
<td>The target port</td>
</tr>
</tbody>
</table>

Ref: [https://malware.lu/articles/2013/04/08/apt1-technical-backstage.html](https://malware.lu/articles/2013/04/08/apt1-technical-backstage.html)
...But Finding Interesting Data and Infrastructure Anyway?

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

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

Ref:
https://intelreport.mandiant.com
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 SHERHAR
PUBLISHED: 17:00 EST, 29 December 2015 | UPDATED: 17:00 EST, 29 December 2015

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.

“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 and 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 spys

By SHASHANK SHERHAR
PUBLISHED: 18:30 EST, 31 December 2015 | UPDATED: 18:29 EST, 31 December 2015

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 airmen Ranjith KK, who was honey trapped by Pakistan’s ISI agency via a fake profile on Facebook.

Ref:

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.

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: https://twitter.com/oryxspioenkop/status/677476361880133632?replies_view=true&cursor=AMCUmNbhZgk
Cybersecurity Researchers Are Hunted from All Sides

Written by ANDRADE HISCUTEAN

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 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 Richard 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 BROKAGE
Juan Andres Guerrero-Saade
Kaspersky Lab, USA
Email juan.guerrero@kaspersky.com

ABSTRACT
The top tier of the information security industry has undergone a toxic shift. Information security researchers are increasingly involved in investigating state-sponsored or geopolitically significant threats. As a result, the edifice and community-friendly information security researcher has become the marginalized and often vilified intelligence broker. In many ways, researchers have not come to accept this reality or the consequences it wrought upon them. Similarly, the 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 firms face drastic changes in their role as intelligence brokers. Necessary areas of improvement beyond dispute include the enhancement of geopolitical analysis skills and analytical frameworks, traditional operational security, and strategic decision making based on a political culture where heightened stakes and disproportionate power are significant players. As the new playing field comes into clear view, so will the geopolitical conditions that are its permanent nature. In the face of continuous geopolitical weight and consequences, whose final attribution remains unattainable nation-states, the most capable security researcher among us will need drastic preparations, not only to exist but to survive.

INTRODUCTION – RE-SITUATING OUR CONCEPTUAL COORDINATES
In recent years, the information security industry has undergone a toxic shift as it has embraced “cyberespionage” research. Reports on advanced persistent threats (APTs) and targeted attacks (TAs) have become commonplace offering for high-end outlets and security wannabes alike. But fighting for headlines that accompany nation-state attacks. Through the bushy newsmen often lack the visibility to or expertise to properly analyze an APT campaign, the top-tier firms are here to pin their legitimacy on intelligence reports. Despite the analytical strength and rigor the points towards 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 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 opportunities between the two. The breadth of interactions that occur therein lead us to understand that attacks are not advanced [1], advanced attacks that are not persistent, widely distributed attacks intended for a specific target, and targeted attacks with the intention of reaching a wider audience. APT is in the genetic material of all attacks that are not targeted at the victim.[2]

Similarly, in-network political aspirations are widely known in the context of nation-states, and their relationship is often covered by a blanket of darkness. Similarly, it is generally believed that the standards and protocols in espionage operations are the same as those of other domains. But this is not the case, and the traditional view of espionage operations is out of date. This shift has occurred largely due to the increased understanding of the role of intelligence agencies, the nature of their operations, and the methods used to conduct them.

1. With malware reaching new levels in memory and learning, malware operators have found a new way to stay hidden. The use of techniques like “obfuscation,” which allows malware to evade detection by security software, has become increasingly common. This has led to a new threat landscape that is more difficult to detect and respond to. As a result, cybersecurity research is becoming more important than ever before.

References:
- http://motherboard.vice.com/read/cybersecurity-researchers-are-hunted-from-all-sides
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