Journal of Strategic Security

Volume 6
Number 5 *Volume 6, No. 3, Fall 2013*
Supplement: Ninth Annual IAFIE Conference: Expanding the Frontiers of Intelligence Education

Article 21

Teaching about 'Area 51'? How to Cover Secret Government Technology and Capabilities in Intelligence Studies Courses

Armin Krishnan
The University of Texas at El Paso

pp. 187-196

Teaching about 'Area 51'? How to Cover Secret Government Technology and Capabilities in Intelligence Studies Courses

Armin Krishnan

Introduction

While there is a wealth of excellent standard literature available specializing on intelligence analysis and how intelligence feeds into foreign policy, which has helped to turn intelligence studies from a fringe subject into a legitimate and serious academic discipline, there are still aspects of intelligence that are notoriously difficult to cover in public university courses, but which are also of enormous importance for understanding intelligence. One problem is presented in the discussion of covert action and its current role in U.S. foreign policy, as covert action is always controversial and not without good reason subjected to a lot of secrecy, which always invites a lot of criticism and speculation. Similar is the situation with respect to secret government technology and certain methods used for the collection and analysis of intelligence. Although there is some good knowledge in the public domain about many aspects of Technical Intelligence (TECHINT) from earlier decades, there is great scarcity with respect to official information on current capabilities for technical collection and analysis. Even excellent primers on U.S. intelligence such as Jeffrey Richelson's *The US Intelligence Community* are very sketchy with respect to collection systems that are currently in use by the U.S. government.[1]

The problem is that the U.S. Government does not – in some cases – even acknowledge the existence of certain collection systems and methods. Nothing epitomizes the extreme secrecy in the field of secret weapons and secret intelligence capabilities more than the Nevada Test Site, known to the public as *Area-51* or *Dreamland*, where some revolutionary intelligence platforms have been developed. In almost sixty years of secret testing and operations conducted on the Nevada Test Site there has not been a single whistleblower revealing current activities, whose credentials can be verified. The super-secret Area 51 may be ironically just the tip of the iceberg of a whole clandestine world of secret government technology development. Several journalists, researchers, and scholars have pointed to existence of a 'black world' of secret sites, secret projects, secret programs, and secret technology development that has been mushrooming at a constant pace since the 1950s and which has come to consume at least ten percent of the U.S. defense budget.[2] Some estimates are substantially higher.[3] It is no longer possible to simply ignore the 'black world' of secret U.S. government technology development and usage without arriving at a very incomplete understanding of U.S. intelligence capabilities. Nevertheless, one has to ask the question: is it even possible to teach about Area 51 without drifting too much into 'X-Files' territory?

[1] Richelson, Jeffrey, *The US Intelligence Community* (Boulder: Westview Press, 2011).
[2] Paglen, Trevor, *Blank Spots on the Map: The Dark Geography of the Pentagon's Secret World* (New York: New American Library, 2010), 182.
[3] According to a report by the DoD Inspector General, an audit of the Pentagon's budget for Fiscal Year 1999 indicated that $2.3 trillion dollars in accounting items out of an overall of $6.9 trillion "were not supported by adequate audit trails or sufficient evidence to determine their validity." Even if most of the $2.3 trillion can be written off due to waste, corruption, and poor accounting practices, one has to wonder how much of the money was used for funding highly classified technology development projects or 'black' operations. 'Audit Report: Report Number D-2000-091', *U.S. Department of Defense Office of the Inspector General* (25 February 2000), 8.

It is the contention of this paper that it is indeed possible to teach about secret government technology in a serious manner and that a serious discussion of a phenomenon such as Area 51 is indeed stimulating and beneficial for students of U.S. intelligence. Since there is not much readily available literature on current capabilities and sometimes deliberate deception on part of the government, one has to be creative in terms of finding relevant information from a wide range of open sources and in terms of putting the material together in a way that makes sure some inevitable speculations have at least a firm grounding in known facts and are based on good analysis. It is also crucial to always communicate to students how reliable the information is and where it comes from. In other words, researching and teaching about secret technology requires a mindset and methodologies based on open source intelligence analysis.

The Government Couldn't Keep a Secret, Right?

There is the misperception, which is continuously reinforced and perpetuated by politicians and the media, that nothing leaks as badly as Washington and that there are no real secrets. The government is believed to be generally incompetent to protect its greatest secrets and that all secrets eventually reach the public because of leakers, whistle-blowers, and investigative journalists busying themselves with undermining the very elaborate and very expensive machinery of government secrecy.[4] This might be true in the sense that a lot of classified information gets eventually leaked, mostly for political purposes and often by the sitting administration itself, but it is definitely not true when it comes to development and operation of secret technical intelligence collection systems and methods. These are classified 'above' Top Secret and are subjected to only minimal Congressional oversight. People are given access to this information only on a need-to-know basis and only after they have been carefully vetted. They have to sign a non-disclosure agreement and would face up to thirty years in prison if they would make unauthorized disclosures of sensitive information. It is no surprise that leaks to the public about highly classified current technical collection systems, operations, and other sensitive intelligence information are extremely rare.

Secret government technology development programs are typically so-called Special Access Programs (SAPs) that employ special security measures and have substantially reduced oversight mechanisms.[5] The Commission on government secrecy headed by Senator Patrick Moynihan revealed: "Special access programs can concern research, development, and acquisition activities; intelligence (including covert action); or military operations."[6] The Central Intelligence Agency (CIA) calls their 'deep black' programs Controlled Access Programs (CAPs). Any information related to sources and methods is classified Top Secret Sensitive Compartmented Information with a codename that identifies the particular compartment (TS SCI codename). Very few people within the U.S. Government and the military-industrial complex, called 'Super-Users,' have access to all information on a compartmentalized program. The government will usually not comment on SAPs, although their existence might be known to the

[4] The U.S. government spent $11.36 billion dollars on the proper classification, handling, and protection of government secrets in 2011. '2011 Cost Report,' *Information Security Oversight Office* (20 June 2012): 2, available at: *http://www.archives.gov/isoo/reports/2011-cost-report.pdf*.
[5] Sweetman, Bill, *Lockheed Stealth* (St. Paul: Zenith Press, 2004), 29.
[6] 'Report of the Commission on Protecting and Reducing Government Secrecy' (Washington, D.C.: U.S. Congress, 1997), p. XXVIII.

http://scholarcommons.usf.edu/jss/vol6/iss5/21
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.19

public, as they are identified by their program names in official budgets. However, few specifics about these programs would be released other than their name and general purpose. In addition, there are 'black' programs that are not identified in official budgets and which are hidden in other budget items. Based on the discrepancies in the overall Department of Defense (DoD) budget it has been calculated that there was $56 billion dollar black budget in 2011, which financed highly sensitive weapons development programs, as well as intelligence programs.[7]

These 'black' programs are known as Unacknowledged SAPs/CAPs, in which cases the government will publicly deny the existence of these programs. For this end government agencies and contractors are authorized to employ cover stories to hide these programs, usually in less classified or public programs of a different purpose. The use of the National Aeronautics and Space Administration's (NASA) *Discoverer* program for concealing the real purpose of testing and deploying the *Corona* satellites comes to mind. In other cases the intelligence community relies largely on private corporations, on front companies, and on other cut-outs. A very famous example that shows the great lengths to which intelligence agencies go protecting special collection operations is of course Project *Azorian* or the salvage operation of the Soviet missile submarine K-129. The operation used Howard Hughes and his company as a cut-out and relied on a sophisticated cover story that disguised the operation as a deep sea mining effort.[8]

Interestingly, the efforts of keeping intelligence activities secret do not stop with SAPs/CAPs: some programs are even more secretive. These are so-called 'waived' USAPs/UCAPs/SCI programs, which may be exempted from being even reported to Congress. For example, it is believed that the National Security Agency's (NSA) domestic surveillance program codenamed *Stellar Wind* is a waived SCI program that does not appear on any public budget and may be only visible to the 'Gang of Eight'. Even the 'Gang of Eight' might not be given many details, nor would this very small group of people be able to exercise effective oversight, considering that alone the list of programs with special access controls regularly provided to Congress is 300 pages long. According to the Moynihan report from 1997, "[t]here are 150 DoD-approved SAPs…down from 200 in the late 1980s, and roughly 300 SCI compartments, compared with an estimated 800 in the late 1980s." These numbers do not even include any sub-compartments, in which further and different programs could be hidden. No human being would have even the time to study all or even any of these programs in detail. According to remarks by DNI James Clapper, "[t]here is only one entity in the entire universe that has visibility on all SAPs – that's God."[9]

Overall it can be said that the U.S. government is not only able to keep secrets, but has a very impressive track record keeping secrets. Some 'black' intelligence and weapons development programs were successfully kept from the public for decades. These very basic observations about the machinery and effectiveness of government secrecy is extremely important for arriving at a much better understanding of current U.S. intelligence capabilities and methods.

---

[7] Adam Rawnsley, 'Go Inside the $56 Billion "Black" Budget', *Wired* (18 February 2011), available at: *http://www.wired.com/dangerroom/2011/02/go-inside-the-56-billion-black-budget/.*

[8] Polmar, Norman and Michael White, *Project Azorian: The CIA and the Raising of the K-129* (Annapolis: Naval Institute Press, 2010).

[9] Priest, Dana and William M. Arkin, *Top Secret America: The Rise of the New American Security State* (New York: little, Brown, and Company, 2010), 27.

What to Include in a Course on Technical Intelligence Collection and Analysis

Technical collection and analysis disciplines have evolved over the decades and have grown in number. More and more 'INTs' have been added to the arsenal of collection methods. A course on technical intelligence collection should include not only the traditional disciplines of Signals Intelligence (SIGINT) and Imagery Intelligence (IMINT), but also some new and emerging disciplines, methods, and technologies, which shall be briefly outlined below.

SIGINT

It is the oldest and most established technical collection discipline with a history of almost 150 years or even thousands of years if one includes Ancient methods for hiding and enciphering communications. SIGINT has evolved from merely tapping telegraph lines and from traditional code breaking to a technologically highly sophisticated effort of systematically monitoring communications and traffic, as well as other signals around the world, including the capability of precisely locating transmitters for targeting purposes and deriving other technical information on transmitters. The biggest problem with respect to teaching SIGINT is that there is very little good literature that deals with current SIGINT capabilities and methods. In particular, the available literature on contemporary SIGINT organizations and operations has almost nothing to say about current code breaking practices or methods. Information on current SIGINT collection activities is also very limited.

IMINT

Imagery intelligence is the other established technical collection discipline, which has a largely known and well-researched history. Many Cold War collection systems and operations have been declassified, most importantly the Corona Project and Hexagon documents. There are many excellent case studies on the uses of imagery during the Cold War period, such as the role of imagery intelligence during the Cuban Missile Crisis or the uses and limitations of imagery during the 1970s Strategic Arms Limitations Talks. Where it gets frustrating in terms of available literature is a lack of good literature on imagery analysis techniques for national security, as well as with respect to currently available collection systems such the newest generation of earth observation satellites and their capabilities. For example, the Undersecretary for Intelligence Michael Vickers has recently hinted that the new spy satellites would be "the most significant change to our overhead architecture in at least three decades".[10] Unfortunately for us there is no further official information available as to why the new capability would be so revolutionary.

MASINT (Measurement and Signature Intelligence)

Over the last ten years MASINT has emerged from being a minor contributor of intelligence to a major technical collection discipline, which already overlaps with and supplants the traditional SIGINT and IMINT disciplines. MASINT is difficult to teach to students in general terms because it consists of a large number of different types of sensors and different methods for

[10] David Barton, 'Mike Vickers: U.S. Has New Spy Satellites, Biggest Advance in 30 Years,' *ExecutiveGov.com* (12 October 2012), available at: *http://www.executivegov.com/2012/10/mike-vickers-u-s-has-new-spy-satellites-biggest-advance-in-30-years/.*

http://scholarcommons.usf.edu/jss/vol6/iss5/21
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.19

analyzing complex sensor data. So it is crucial to outline some of the physical principles behind MASINT collection systems and analysis techniques, as well as explaining MASINT's growing contribution to some of the biggest current challenges for U.S. intelligence, namely counter-proliferation (WMD detection), counterterrorism, and finding deeply buried underground facilities. There are also several historical examples that have a continuing relevance for the discipline: the Long Range Detection Program, DSP, and SOSUS.

Technical OSINT (Open Source Intelligence)

OSINT contributes most in terms of quantity to US intelligence collection. While OSINT is mostly about the collection and analysis of published or broadcast material, there is also a technical side to OSINT and this is at the current time primarily commercial imagery, navigation, and mapping technology, as well as new computerized methods for tracking and analysis, which is known as Geographic Information Systems (GIS). This subject is very important because of the widespread use of commercial imagery and GIS by a large number of federal agencies and private businesses and it is also relatively unproblematic to cover because of the massive amount of public literature.

HACKINT (Hacker Intelligence)

The collection of intelligence through computer network attacks has become the cutting-edge of SIGINT and has enabled fairly new ways of acquiring intelligence on a range of state and non-state targets. Sometimes termed 'cyber espionage' or even 'cyberwar' government hackers have been highly successful in attacking foreign computer networks and in downloading sensitive information. It is known that Chinese hackers were able to steal a terabyte of data relating to the F-35 project from defense contractor Lockheed Martin. Although it is rarely officially acknowledged, the NSA is engaged in similar offensive cyber operations and might be actually ahead of the Chinese in the field of cyber espionage. Students shall understand the role of intelligence services in the cyber domain, as well as some of the technical and intelligence methods used for gaining access to sensitive data such as the use of hacker tools (viruses, worms, Trojans, botnets), as well as black bag jobs, 'social engineering,' hardware viruses and backdoors built into devices and electronic components, and the use of malicious insiders. The available literature on the general subject matter is extensive, but very little of the literature has anything to say about U.S. government cyber espionage and other offensive cyber operations, which makes it tricky to understand current U.S. capabilities and collection activities in this field.

Secret Aerospace Technology, Robotics, Artificial Intelligence (AI), and Nano-Technology (NT)

There is a long history of secret development of revolutionary aerospace systems, most importantly the U-2, the SR-71, and the stealth fighter, but information about the Pentagon's secret space program and a potential successor system to the SR-71 (for some time known as *Aurora*) are sketchy at best and unconfirmed. Nevertheless, it is absolutely certain that the Pentagon is spending substantial amounts of money in developing revolutionary aerospace systems, some of which are probably operational and used in crisis situations and wartime.[11]

[11] A UK MoD report claims: "Research and development on hypersonic technology is expanding, principally in the USA. The projected (USAF) priority plan is to produce unpiloted air-breathing aircraft with a Mach 8-12 capability and transatmospheric vehicles which can operate between the upper air-breathing and sub-orbital flight regimes, as

Current robotic collection systems such as the *Global Hawk* drones are only at the beginning of a wider technological revolution that could fundamentally transform human society and warfare in the 21st century. There are not many limitations in terms of size, allowing theoretically developing robots and sensors of a microscopic size. Robotic systems can also more easily combine a intelligence, surveillance, and reconnaissance function with an operations or combat function, as can be already seen in the *Predator* drone. A lot of R&D in the fields of robotics, AI, and NT is highly classified, in particular hypersonic and stealth drones, micro-drones and nano-scale systems, but there is still enough material in the public domain for giving students some ideas about the future potentials of these technologies.

Automated Processing, Analysis, and Surveillance Technology

This topic is difficult to cover, but is nevertheless too important to simply exclude it from any overview course on TECHINT. Since technical collection enables the systematic collection of vast volumes of data, there has been a growing need for the automated processing and analysis of this data. There are also new types of surveillance and monitoring systems that are highly automated and that can flag suspicious individuals, communications, activities, and threats to analysts. Basic methods include traffic analysis, speech recognition, machine translation, data-mining, and link-analysis. Some of the methods and tools are in the public domain. From unclassified documents related to Echelon it seems that the IC used voice recognition and machine translation since the 1970s.[12] Various sources indicate that the NSA can monitor 1.5 billion communications a day by relying on voice recognition, machine translation, word-spotting, and context-spotting with the help of weekly updated dictionaries. It is very hard to understand capabilities in this field because of the very rapid technological development and the scarcity of information on automated signals and imagery processing within the IC.

How to Teach about Secret Government Technology

A course on technical intelligence cannot rely exclusively on official documentation since most of it is classified and not available for use in an academic program. It is therefore important to be creative in terms of finding relevant and trustable sources and in terms of presenting these materials to the students. In a field like intelligence deception is the normal mode of operation. As a result, there can be very few certainties in intelligence studies even with respect to the historical records of intelligence services since they not only conceal their current activities, but even try to manipulate their historical records in order to shape their public image and in order to permanently cover up controversial activities or particular cases of incompetence or corruption. While little is certain, it is absolutely crucial to communicate to the students where there is more or where there is less certainty and to indicate to them particular sources and the varying degrees of reliability of available information. The main sources on an overview course on technical intelligence collection would mainly comprise of historical literature and relevant declassified documentation. Also important for such a course would be technical and scientific literature that discusses some of the engineering and scientific foundations of technical intelligence collection systems and analysis methods. In addition, there is unclassified literature that deals with certain

---

well as highly supersonic vehicles at Mach 4 to 6." Meirion Jones, 'Report Fuels Spy Plane Theories,' *BBC News* (14 June 2006), available at: *http://news.bbc.co.uk/2/hi/programmes/newsnight/5079044.stm*.

[12] 'Echelon Automated Data Processing Equipment,' ca. 1976-82, available at: *http://cryptome.org/jya/echelon-adpe.htm*.

http://scholarcommons.usf.edu/jss/vol6/iss5/21
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.19

unclassified aspects of TECHINT, which outlines particular challenges for technical collection, or which provides particular visions or goals for future capabilities. Finally, it is crucial not to disregard leaked information and information that comes from whistleblowers or former insiders. Equally important is information from official foreign sources, such as parliamentary investigations and reports. An important example is the 1999 Europe Union (EU) report on Echelon.[13]

Historical Cases

It is always good to start with information that is best documented and therefore most reliable. Some historical focus gives the students a better understanding and appreciation of the technological evolution that laid the foundations for today's capabilities. For example, there is a large amount of excellent literature on code breaking during the Second World War, in particular on the history of the allied achievements of breaking Enigma and Purple. Many technical aspects of both the Enigma machine are described in detail, as well as the methods and activities that contributed to breaking the Enigma cipher. Of course, code breaking has not really stopped with the Second World War, nor has it remained unchanged. In other words, going into the history of code breaking is beneficial for the students, but they also need to be aware of certain more recent breakthroughs in cryptology and more current approaches of collecting and processing signals. This sometimes requires venturing into more unconventional territory in terms of sources than the official histories of code breaking that stop with the years after the Second World, Venona being the last major declassified U.S. code breaking effort.

Physics and Engineering Principles

Many physical and engineering principles and physical limitations of collection systems are in the public domain and can be utilized for a TECHINT course. The intelligence studies literature includes some notable contributions that describe the engineering aspects of some current systems such as Synthetic Aperture Radar or methods such as spectral sensing, which are also used for a range of civilian research applications. An excellent primer in this respect is Robert Clark's The Technical Collection of Intelligence where he outlines many current collection technologies and the underlying physical principles.[14] There is a tremendous amount of literature on computer hacking, computer crime, and cyber espionage that does not necessarily deal with national security, but which is equally for this domain, as the main principles and issues are similar in the civilian world.

New Technological Challenges, Visions, and Goals

For getting a better feeling for what kind of capabilities are desired or might be available in the future it is always good to look at agency websites that publish vision and planning documents, including professional or in-house journals as far as they are accessible to the public. This type of literature provides a better understanding of what the agencies consider to be their main challenges and even how they intend to overcome these challenges. Although there is no classified information included in such publications, they do give insights about current capabilities as sometimes existing capabilities are described as aspirational, which allows people

[13] 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)),' *European Parliament* (22 July 2001).
[14] Clark, Robert M., *The Technical Collection of Intelligence* (Washington: CQ Press, 2011).

with access to this classified information to openly write about them without giving away any secrets. Another good source of information on currently developed revolutionary technology is Defense Advanced Research Projects Agency (DARPA), as the agency publishes tenders for projects that it intends to fund, including some technological specifications for these projects. For example, DARPA has been funding brain mapping research for over a decade, which could ultimately lead to capability of brain reading that could give intelligence agencies direct access to the brains of our opponents.[15] The thoughts and dreams of a subject could be decoded. As far out as this sounds, it is very likely that some limited capability in this regard already exists, considering progress made in public research.[16]

Whistleblowers and Leaks

Some of the most revealing and potentially most valuable information comes from current or former insiders, who leak information to the public as whistleblowers to expose wrongdoing or to affect a change in policy concerning certain activities or to make technologies that are kept secret available to the general public. Since it is usually impossible to understand the motivation of whistleblowers and leakers and since it is difficult to verify the information, one has to be very careful with respect to leaked information. At the same time, it is absurd to disregard information just because it has been leaked. For example, historians writing about the Vietnam War could not possibly ignore the leaked Pentagon Papers, no matter how they feel about Daniel Ellsberg and his intentions. The same applies to 'WikiLeaker' Bradley Manning and thousands of other former insiders, who decided to break their secrecy oath for whatever reason. As scholars, researchers, and educators we have to take leaked information seriously until it is proven to be inaccurate. One way of overcoming uncertainty is to rate sources to understand the value of the information coming from them. Anonymous leaks have to be distrusted more than leaks from an identified source, and an identified source with verifiable credentials is more trustworthy than a source without verifiable credentials. As everything in the intelligence world is so highly compartmentalized, even former insiders can only provide small pieces of the puzzle and they may themselves be manipulated into unwittingly planting disinformation. One should always try to corroborate information from leaks and whistleblowers with information from other sources. Obviously, the account of a single whistleblower or from a single leak has to be distrusted, but the accounts of many whistleblowers can cumulatively add up to a more coherent and more complete picture.

Conclusion

A course on TECHINT can be either very historical, focusing only on technologies and methods that were state of the art 50 or more years ago, or it could be very technical, focusing on the physics and engineering aspects of collection systems and methods of analysis that would provide only a very narrow understanding of TECHINT. For an overview course on current TECHINT capabilities and methods for students in non-technical academic programs I recommend to strike a healthy balance between the history and the science, while also incorporating information that is somewhat outside of the 'regular' intelligence studies literature and possibly at the fringes of the professional and academic literature. Some speculation on

[15] Moreno, Jonathan D., *Mind Wars: Brain Research and National Defense* (New York: Dana Press, 2006), 97-113.
[16] Kathleen Taylor, "Mind Reading Is Possible!," *Salon* (15 December 2012), available at: *http://www.salon.com/2012/12/15/mind_reading_is_possible/.*

http://scholarcommons.usf.edu/jss/vol6/iss5/21
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.19

certain capabilities should not only be considered permissible – to some extent it is simply unavoidable. Apart from the more theoretical and skill-oriented sub-field of intelligence analysis, most aspects of intelligence studies and intelligence history can never claim the same certainty with respects to facts than the natural sciences or even social science disciplines. One has to accept that concealment and deception about collection methods and capabilities is part of the game and that official documentation about current capabilities and operations might only be revealed in twenty-five years from now, if at all. It is just important to indicate to students where the information comes from and to what extent the information can be trusted.
Covering the history and the science/ engineering aspects is quite straight-forward. When it comes to covering current and near future TECHINT capabilities, then I would recommend the following rules of thumb for arriving at a more accurate estimate of what might be technologically possible in today's world.

1. Current or future intelligence capabilities are more advanced than older and known systems for technical collection and analysis. This should be obvious. Everything that could be done some decades ago can be done today much better since technology has advanced and continues to advance. For example, biometrical face recognition systems for Closed Circuit Television (CCTV) that were first deployed in London's Borough of Newbury in 2002 and which disappointed in their lacking ability of identifying any criminals known to be living in that area, have probably improved by a factor of a hundred times over the last decade. From this perspective a nationwide system utilizing biometrics for tracking people on watch lists is probably not that far away.[17]

2. If a certain technology is available in the civilian world, the U.S. government can be expected to have a more advanced version. This is also a 'no-brainer'. No private business can match the resources of the U.S. government for the R&D of national security relevant technology. Whatever gets deployed in the private sector in the security field is naturally inferior to what the government has. Looking at commercial technologies allows us to extrapolate from the known public sector technology to whatever technology the government may have available. If a private entrepreneur such as Richard Branson can build a space plane with some moderate investment than one can be fairly certain that the U.S. government already has the capability of a 'Common Aero Vehicle' that can reach any point on earth in just a few hours.

3. If a certain technology is available to or used by foreign governments, the U.S. government will also have that capability. While other governments are hardly less secretive about their secret weapons and intelligence systems, there is sometimes more information available on foreign systems or capabilities than on U.S. systems and capabilities. This makes it worthwhile to look at what other nations have come up with. Surely, if other governments have it, the U.S. government will have a deluxe version. For example, the Russians and the Chinese have built submarine bases with undersea entrances. It is a reasonable assumption that the U.S. Navy also has secret submarine

[17] Michael Kelley, 'The FBI's Nationwide Facial Recognition System Ends Anonymity as We Know It,' *Business Insider* (10 September 2012), available at: *http://www.businessinsider.com/the-fbis-nationwide-facial-recognition-system-2012-9*.

bases, possibly undersea bases, which are used for highly classified intelligence operations.[18]

4. If a certain technology or capability is currently presented as theoretical, chances are it already exists or may exist in the foreseeable future. There is a whole range of intelligence technologies that are described as aspirational like: 'it would be good if we could look hundreds of feet underground in order to find deeply buried facilities.' It is quite possible that High Frequency Active Auroral Research Program (HAARP) in Alaska can use ELF/VLF radio waves reflected from the ionosphere for detecting deeply buried facilities around the world.[19] This is, of course, speculation, but there are many indicators pointing in the direction that HAARP has an operational function, be it communication with submerged submarines around the world or be it missile defense. Even if HAARP lacks the capability of looking underground, the use of ELF/VLF waves for this purpose, as well as other methods like the detection of electromagnetic anomalies, could be available for this end.

From my limited experience teaching an overview course on TECHINT I can say that students tend to be fascinated by topics such as the extremely secretive development of revolutionary intelligence capabilities. It has become a huge part of what the IC does. For the instructor and students alike it is great fun to practice analytical skills, to dig up snippets of information here and there, and to ponder the possibilities.

[18] Sauder, Richard, *Underwater and Underground Bases* (Kempton: Adventures Unlimited Press, 2001), 143-181.
[19] David Hambling, 'Pentagon's Scientists Target Iran's Nuclear Mole Men', *Wired* (12 January 2010), available at: *http://www.wired.com/dangerroom/2010/01/irans-nuclear-molemen/.*

http://scholarcommons.usf.edu/jss/vol6/iss5/21
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.19