Wikileaks: causes and consequences

military-Earth thinking notebook

le Lieutenant-colonel LEGRAND

Published on 02/08/2018

Histoire & stratégie

On April 25, the New York Times **published an article analyzing documents classified as "secret" by the DoD [1]. These documents, known as DAB[2], are reports on the various detainees held in Guantanamo Bay prison between 2002 and early 2009. The Pentagon immediately condemned the revelation of this information, highlighting in particular the imperatives of national security. The source of these leaks is once again the "wikileaks" website, which had already stunned the world at the end of July 2010 by releasing 75,000 pages of classified documents relating to the activities of American forces in Afghanistan.**

[1] Department of Defense

[2] Detainee's Assessment briefs

The documents, stolen by someone with the required clearance, then revealed daily reports from several units, giving a clear picture of US operations from 2004 to 2009. They also included reports revealing American frustration with Pakistan's secret assistance to the insurgents. The documents revealed dates, times, unit names, geographic locations, and sometimes the names of Afghans who had worked with the Americans. While the Pentagon warned the site to remove these documents and not to disclose 15,000 other classified documents that would endanger not only Americans but also many Afghans, WikiLeaks reiterated in October 2010, releasing nearly 400,000 pages of classified documents about the Iraq war. Finally, in December 2010, the site revealed numerous diplomatic cables exchanged between the State Department and its diplomatic missions around the world.

It was finally only thanks to a denunciation that we learned that the leaks were the work of a Private First Class soldier, Bradley Manning,a former intelligenceanalyst at theArmy intelligence analyst Bradley Manning, who is already suspected of having delivered to the site a video showing an Apache helicopter killing two Reuters Agency employees.

Under what conditions could a non-commissioned soldier have had access to and stolen so many classified documents?

After an analysis of the causes [1], this article will develop the main consequences of this "event".

Causes of the Wikileaks affair

- Background
  - Manning, 23, unlikely culprit?

Bradley E. Manning, a simple non-commissioned officer, was trained as an intelligence analyst and had Top Secret clearance: if this may already seem surprising to a Frenchman, it should be pointed out that for the Army, engaged in Iraq and Afghanistan, this isa fairly common case, given the enormous need for analysts.

Deployed to Iraq in 2009 with the 2nd BCT of the ^{10th} Mountain^{Division}, Manning is therefore not a spy but a simple Private First Class who operated from a small advanced camp in Iraq. Many voices have been raised in the United States to denounce the fact that such a young soldier could, from the middle of the desert and with the help of only a few computers, access and then download so many classified documents. Second, how could he remain active for so long without being suspected? Indeed, his arrest was only possible thanks to the testimony of an ex-computer hacker[2], with whom Manning confided.

But in today's modern military world, where information plays a vital role, it seems easier than one might think, according to the testimony of many intelligence officials, to access and disseminate classified documents.

- A facilitating job

Manning's job was to ensure that the other intelligence analysts in his group had access to all necessary information, including incoming intelligence flows, from around the world. This included access to the JWICS[3] network, the DoD network carrying Top Secret classified information. Manning also had access to another information network called SIPRNet [4], a secret classified network created in 1995, originally intended for the Pentagon but open to different departments and agencies since the attacks of September 11, 2001. This was in fact one of the major advances made in the field of intelligence sharing under the impetus of the September 11th Commission, which had drawn lessons from the terrorist attacks, particularly in the field of access to inter-agency intelligence.

By making requests using key words and having sufficient knowledge of the usual nomenclature, any intelligence analyst can thus have access, from anywhere, to any information of his or her level of clearance. However, Top Secret level information or intelligence cannot normally be retrieved from computers easily. In order to transfer information from the IRRSNet to unclassified networks, analysts such as Manning use proprietary computers called SNAP[5]. About 1,500 SNAP computers are deployed in Iraq and Afghanistan, according to the company that manufactures them, TeleCommunications Systems.

According to one user of the system, SNAP allows the user to securely transfer data from a classified network to an unclassified network and vice versa. The user can then transfer the data to removable media, burn it to a CD or simply send it by e-mail. It is also essential to know that diplomatic cables are transmitted by e-mail over secure networks and stored on servers until they are destroyed [6]. 6] Cables and incident reports from the field are stored on servers as PST files[7], an e-mail archive that Microsoft Outlook uses to compress and store data.

- How Was Manning able to get access to the diplomatic cables? They are actually transmitted by e-mail as a PDF file on a State Department network called ClassNet, but stored as PST files on servers that can be accessed by an authorized analyst with a query. Thus, if Manning's unit needed to know whether insurgents were procuring new weapons from Iran, the information could be contained in a diplomatic cable. An analyst could then download a PST file containing the cables, open them, transfer them to a SNAP computer, place them on removable media, and then erase the file movement history on the server. It should be remembered that during the Iraq war, downloads of huge amounts of data were commonplace and it is difficult to detect suspicious conduct in such a context.

Manning is believed to have started feeding information to WikiLeaks in the fall of 2009 and his access to the computers was only cut off at the end of May 2010. How could Manning have been able to download the files for so long without any security system raising an alarm?

Yet such a system existed but was simply not activated.

- The flaws in the security system
- An alerting software was in place but disabled. When BAE Systems and its subcontractor Mc Afee were chosen in 2006 to install security on thousands of DoD computers, the technology was designed to stop external threats: foreign intelligence officers, hackers or hackers wanting to spread viruses or malware across the Department's networks.

The HBSS[8] software established digital links between network security personnel and the classified computers used by the troops and intelligence analysts. This allowed security personnel to remotely monitor the computers to ensure that the antivirus database was up to date and that there was no malware on the computers.

DoD officials were so obsessed with intrusions that software capable of alerting authorities about large downloads was added to HBSS in 2008, but never authorized and activated according to an official source.

The McAfee software was part of a broader enhancement aimed at giving security officials the ability to disable data ports on remote computers in the event of a malware attack. The Pentagon has yet to confirm whether HBSS was in the computer used by the suspect in this case, PFC Bradley Manning.

- A focus on outside threats

Experts marveled that State Department cables are being spread over the Internet by the fact that one person could have stolen so much SIPRNet information without triggering an alert throughout the network. Some monitoring systems were in place, but only in a few places. Moreover, even if the HBSS software was installed on Manning's computer, it made no difference because data loss detection was not activated. Security had in fact been focused on external threats since the 2008 attacks on US Central Command: a digital bridgehead had been introduced from which data could be transmitted to servers controlled by foreign services. The Pentagon launched Operation Buckshot Yankeeto solve the problem. Many security officials wanted the ability to remotely disable removable media ports, particularly USB ports. Mc Afee designed an add-on to HBSS that would allow the ports to be disabled. However, because Americans were focused on external threats, the download alert software was not enabled.

One of the many questions raised by this affair could be the one asked by a senior intelligence official: "Should a first class infantry $^{\text{battalion}}$ in Iraq be able to access cables from Eastern Europe? SIPRNet, after 11 September 2001, was gradually transformed by the American government into a forum open to authorised individuals so that they could share intelligence and reflect and then exchange by e-mail on concrete intelligence problems. SIPRNet has thus become a kind of equivalent of a classified Internet, supplemented by sites.

The consequences

- Immediate action
- As the WikiLeaks affair highlighted several security failures, the Army took a series of firm measures at the end of 2010 to prevent this from happening again.

- The Army has asked all units to re-evaluate their security measures and to limit administrator rights.. They should also disable the CD and USB ports, so as not to allow data to be copied too easily. Non-commissioned members should only have access to data that is not very confidential;

- The Army has reiterated the prohibition on carrying any personal electronic devices or software in a government compound.. In addition, soldiers must use only the prescribed methods for any transfer of data between computers or networks of different classification;

- Updated security regulations were published in October 2010, highlighting a list of indicators that could reveal a risk of espionage, terrorism and internal threats.. Known as "AR 381-12, Subversion and Espionage against the US Army", it has been applicable since 4 November 2010. The behavioral signs listed in the manual were taken from actual facts, soldiers or employees of the Army who illegally disclosed information;

- All units must now carry out unannounced checks.s, especially in the most sensitive facilities. Units are also required to review how they combat internal threats and enforce regulatory procedures. Corps commanders are required to send a report on a regular basis;

- The technical measures envisaged

- A new role for HBSS?

The WikiLeaks affair has prompted the Pentagon to give HBSS a new role, also to combat internal threats.

It is likely that HBSS and data loss prevention software will be among the main points of the OBAMA administration's plan following the WikiLeaks case. In its only detailed commentary on the case, the Pentagon pointed out that HBSS is now installed on 60% of DoD computers connected to the network from which the leak came, the IPSRNet.

Even before the latest WikiLeaks incident , defense officials were developing a request for proposals to determine the next supplier for HBSS's successor, with the current contract expiring in August 2011. The measures taken by the White House, in addition to prevention against data loss, should focus on strengthening security: access authentication, alert system and technologies to compartmentalize access to secret information, without compromising the intelligence-sharing arrangements in place since September 11, 2001.. In fact, WikiLeaks is only accelerating measures that are already being considered.

After the last WikiLeaks incident , the Pentagon announced that it had extended port control software to Central Command computers. However, for many, disabling USB ports or CD-DVD drives does not seem to be the preferred option: they are indeed necessary for many people to do their jobs. Indeed, the three main networks of the intelligence community[9] s are separated from each other and intelligence analysts necessarily need to move unclassified data to, for example, a classified report.

- Intelligence sharing in question?

Many senior intelligence officials still fear an over-reaction to the WikiLeaks affair, and in particular that all the progress made in terms of intelligence sharing will be called into question. In the intelligence community in general, many testimonies referred to the fear of a return to the days when one had to "show a white paw" for the slightest request. Although this does not seem to be the case, many military officials and industrialists nevertheless expect changes in the way intelligence is shared. For example, the State Department has almost immediately closed its SIPRNet sites, which is only a temporary solution as analysts need access to it for their reports.

Statements by U.S. officials suggest that more attention will be paid to those who use SIPRNet and especially how they use it. Protecting secrets without sacrificing intelligence sharing will require technical and political solutions that, in the long run, will be costly, according to one American general.

One such solution could come from the DARPA [10] agency, which recently announced an initiative to develop software that would identify and expel people stealing secrets from classified networks. The Cyber Insider Threat program or CINDER would increase the accuracy, rate and speed of detection of internal threats and prevent adversaries from operating with impunity in military and government networks. The program, led by former hacker Peiter "Mudge" ZATKO, now head of DARPA, was in the making but has become a priority since the WikiLeaks affair.

- A disturbing case?
- Or an inconvenient set of cases?

The WikiLeaks affair has over time become WikiLeaks "business": the site has made the front page of the major newspapers about every two months since July 2010, each time plunging the Pentagon and the White House into embarrassment, so much so that the revelations are so juicy.

Moreover, the leaks revealed by WikiLeaks come in a context already marked by other recent cases, which have seriously damaged the credibility of the American intelligence services. Thus, while the affair of the classified documents revealed by this site was already taking on considerable proportions in 2010, another affair, the planned publication of 'Operation Dark Heart,' sowed furthertrouble in Washington. The book on Afghanistan was written by Reserve Lieutenant Colonel Anthony Shaffer while he was serving as an analyst with the Defense Intelligence Agency. Shaffer deployed to Afghanistan for five months to the US base at Bagram in 2003. After losing his DIA accreditation, he was revoked following several security breach cases and currently holds a research position at the Center for Advanced Defense Studies.

Although approved by many official readers, other readers from different intelligence agencies estimated that the book had more than 200 passages containing protected information. According to the director of the DIA, revelations about clandestine operations in Afghanistan could thus be detrimental to national security. In particular, the book revealed compromising details, such as the names of CIA or NSA agents operating in Afghanistan as well as US espionage networks in Pakistan.

The Pentagon bought back almost all 10,000 copies in order to destroy them, but several dozen unredacted books are still in circulation. Several magazines and newspapers, such as the New York Times, have been able to obtain them via the Internet. In addition, some commentators believe that the Pentagon has given enormous publicity to a book that might otherwise have gone unnoticed?

Another example is another recent series of leaks in the media, which led the director of national intelligence to ask his agents to "shut up". The director, James R. Clapper, said he was worried about the revelations of confidential information in the press.

- A case that sparks passionate debate

The OBAMA administration has certainly severely condemned the leaks of diplomatic telegrams exploited by the WikiLeaks site and published by many international media . Secretary of State Hillary Clinton said that these publications were "an attack not only on American interests" but also "on the international community. But while this case is still far from dividing American opinion, it has nevertheless sparked an often passionate debate, as shown by the many articles and other statements that have appeared in recent months.

Conclusion

The sheer number of documents downloaded, numbering in the hundreds of thousands, by a single young soldier in the ranks, can be explained in part by security breaches that some consider unacceptable. The Americans, traumatised by the events of 11 September 2001, focused on external threats and therefore did not consider it useful to activate existing warning systems. In addition, these cases also brought to light the impressive number of individuals and agencies with access to secure networks [11].

11] The real challenge for the Americans will now be to find the balance between security and the need to provide units with the intelligence they require.

1] These are essentially technical causes.

2] Adrian LAMO

[3] Joint Worldwide Intelligence Communications System

[4] Secure Internet Protocol Router Network

5] IRRS-IPRS Access Point

6] The State Department documents would be stored on the Net Centric Diplomacy Data Base (NCD) on SIPRNet.

7] PST = Personal Storage

[8] Host Based Security System

[9] Non Classified Internet Protocol Router Network; Secret SIPRNet and TOP-Secret Joint Worldwide Intelligence Communications Systems

[10] Defense Advanced Research Projects Agency

11] Nearly 2 million individuals would have access to SIPRNet.

Lieutenant-Colonel Yannick LEGRAND, enlisted in the artillery (reconnaissance officer at 53°RA) was admitted to the Military School of the Technical and Administrative Corps in 1992. During his career, he served in particular at the EAI, then at 44°RT and then at the Intelligence Brigade. He is currently a liaison officer at the United States Army Intelligence Center of Excellence in Fort Huachuca (Arizona). He holds a Master's degree in Political Science and is a former CID intern (2005-2006). He has spent two stints in Kosovo in Pristina (2001-2002) and Novo Selo (2009-2010 Multinational Task Force North ISR BAT Commander).

Title : le Lieutenant-colonel LEGRAND

Author (s) : le Lieutenant-colonel LEGRAND

Release date 12/02/2021