

Deutscher Bundestag
1. Untersuchungsausschuss
26. Aug. 2016

MAT A SV-16.pdf, Blatt 1

Deutscher Bundestag
1. Untersuchungsausschuss
der 18. Wahlperiode

1st Committee of Enquiry
Deutscher Bundestag

MAT A SV-16 / 1

zu A-Drs. 511

James A. Lewis, Center for Strategic and International Studies
September 8, 2016

I would like to thank you for the opportunity to testify. It is an honor and I look forward to your questions and our discussion.

It is understandable that the Bundestag would want to open an enquiry into NSA activities in Germany. Your historical experience is very different from ours. In the 1930s and in the East until 1989, this kind of intelligence was used against your own people rather than as a shield. You think Stasi, but we think Bletchley Park, Enigma and the Battle of Midway. Signals intelligence helped prevent Axis victory in the Second World War and Soviet victory in the Cold War. Signals intelligence still defends the U.S. and our allies from terrorism and resurgent authoritarianism.

When I met with some member of this Committee two years ago, I warned that in starting down this path, they might find more than NSA at the end of it. An accurate enquiry must look at the entire picture. Communication surveillance is a global practice. Most countries conduct domestic surveillance, usually with little oversight or legal constraint. In the capitals of leading economies, such as the U.S. or Germany, we could expect to find at least half a dozen countries attempting to conduct signals intelligence activities. In Washington DC, for example, several nations engage in communications surveillance against American targets.

Espionage and surveillance do not occur in a vacuum but in a larger political and security context. This enquiry must be placed in this larger strategic context. Powerful nations will act to protect their interests, and this includes undertaking intelligence activities. Since all great powers spy, spying in itself says little about the nature of bilateral relationships. Nor does undertaking intelligence activities explain a nation's commitment to civil and political liberties. To accurately assess espionage, we must look at how it is used and what laws shape that use. An accurate assessment will show that like any other tool of governance, espionage can be a shield for democracies or a weapon for dictators.

I had the opportunity to live in a real police state when I was a young diplomat. It was not very pleasant and it involved suppression of the media, opposition political parties, labor unions, and any other potential source of dissent, using a combination of mass surveillance, an exceptionally large security force, a system of block captains to monitor their neighbours, arbitrary detentions and other coercive tactics including the occasional extra-legal execution. It is worth noting that the construction of this police state was assisted by East Germany, along with "advisors" from the Soviet Union, Cuba and other communist countries. Stasi, I believe, provided automated equipment to help track and punish dissidents.

You can still find countries that follow this Leninist model for suppressing political opposition. This desire to stifle dissent is one reason we see powerful objections from some states to the open and free nature of the internet. Attitudes towards free speech are the best indicator of civil liberties and provides a metric by which we can judge espionage, surveillance and the risk of

intelligence operations. Is the political opposition suppressed? Are journalists and opposition leaders murdered, jailed, or forced into exile? Is political material taken by hacking leaked to damage opponents? Is free speech stifled? We all know there are countries where this occurs, but the list of such countries does not include Germany or the U.S., or for that matter any European democracy.

One problem with the public discussion of surveillance is that it has conflated three different kinds of espionage. Governments spy on other nations' military and political leaders. They also spy on foreign intelligence agencies acting in another country. Today, they also spy on borderless jihad. Mass collection is not that useful for the first two categories. It primarily serves counter-terrorism purposes and provides a means of identifying terrorists and their networks.

Having seen at very close range what mass surveillance looks like, neither Germany or the United States engage in it. The idea of a "surveillance state" in a western democracy is a fiction created for political or commercial advantage. There is no such state. The explosion of information created by the internet has immense benefits, but it also created an environment where conspiracy theories, paranoia and falsehood flourish. Our job as analysts is to develop strong, factual methodologies and identify where political or personal agendas shape conclusions in unhelpful ways. Hostility to another country or to political opponents should not color our assessment of surveillance or espionage and the accompanying risks and benefits associated with such programs.

I am not in a position to comment on BND activities, but to assess them, I would use metrics derived from political liberties - liberty of expression and assembly, and the ability to criticize or remove a government. It seems unlikely, despite an immense quantity of leaked documents, that BND activities were used to damage the political opposition, or to suppress the media. Safeguarding these liberties is a crucial concern for all democracies, and Germany already has extensive protections. Oversight of secret activities is essential to reassure the citizens of a democracy that their liberties are not threatened by their own government, but at the same time, Germany must take into account its worsening security situation and the increased danger to its citizens as it considers its intelligence activities. Finding a pragmatic balance between transparency and the safety of citizens should be one of the goals of this effort.

On the issue of the U.S. request that the BND not provide American intelligence to the Bundestag, this is a standard practice among intelligence agencies and essential for cooperation. This practice applies not only between the U.S. and Germany, but to the other nations with whom the U.S. has a cooperative relationship. Equally, the U.S. would not release German intelligence to Congress without the BND's approval, nor would it provide intelligence supplied by any other of our partners without their approval.

The political and security context for espionage is important. We were overconfident after 1989, when some believed that the final defeat of totalitarianism meant the end of history and conflict. Twenty-five years later, democracy is in retreat and on the defensive. It faces complex challenges, some from the political forces created by information technologies and some from

the coercive acts of non-democratic states and groups. It is bitter that we find ourselves again in a struggle to defend democracy, but pretending that this conflict does not exist is damaging.

The security situation for Germany and the U.S. is much worse than it was in 2000 or even 2013. It is easy to blame the Bush Administration and there is no doubt that its many foreign policy errors harmed our security. But even without these American errors, our security would face major challenges. There would be turmoil in the Middle East even without the failed intervention in Iraq. The structure created by the Sykes-Picot agreement was collapsing and the popular uprisings of Arab Spring in the Middle East were unavoidable. Why this occurred is a more complex discussion not really germane to this committee, but the result is that the terrorism problem facing the world is infinitely greater now than anyone expected. Daesh and other terrorist groups are not bound by national borders. They are transnational in recruitment and action. A disaggregated defense split along national lines creates opportunities for them, as we have all seen to our misfortune in Europe.

Similarly, our hopes for close and friendly relations with Russia have been dashed. The course Russia has taken is not what most would have predicted a decade ago. Russian hostility to democratic governance and NATO shapes its policies today as it struggles to reassert its Great-Power status. Russia is engaged in a new, covert political struggle with the West in ways for which we are unprepared. A key part of this involves Russian strategies to split the U.S. and Europe – a long standing Russian goal – and to use media and information technologies to shape public opinion in ways unfavorable to democracy. This includes the use of internet trolls, the creation of government media outlets, subsidies to extremist groups, the manipulation of refugees, leaks of sensitive emails obtained by hacking (which we have seen not only in the U.S., but in Ukraine, Russia itself and perhaps as far back as “Climate-gate”) and of particular interest to this committee, the use of the materials brought by Snowden.

The release of the Snowden material is a major success for the Russian intelligence services. This should not imply that Snowden or his handlers are witting agents of the Russians, merely that their actions have been skillfully exploited by the Russians. The Snowden material has introduced a fundamental inaccuracy into this discussion, since the material being released is shaped to support an intentionally incomplete narrative designed to create the impression of an iniquitous NSA. I am told that other documents taken by Snowden would reveal the activities of foreign intelligence services, information that would dilute or contradict this story. As a result, European perceptions of America intelligence activities are inaccurate and manipulated for political ends.

No doubt the Russians are pleased with their success. Snowden may not have intended to harm Western security but he did so. The best example may be a document taken by Snowden (and published in leading American newspaper) that showed that the NSA monitored the launch sites of Russian strategic nuclear forces. This communications surveillance program had nothing to do with the privacy of American or German citizens and its loss damaged the security of both of our nations.

Russia is America’s equal in signals intelligence, active in Germany and other European countries, and as Crimea shows, hostile to the ideals that have kept Europe in peace for decades.

Russian actors recently penetrated Bundestag networks and its efforts to manipulate American politics are now well known. This too is the context for an enquiry on Snowden and NSA. I would not be surprised if the Bundestag received additional attention from the east as the 2017 elections draw closer.

The Snowden revelations should not have come as a surprise. The internet has never been secure and many countries have taken advantage of this for intelligence purposes to the extent their laws and resources allow. No country is innocent. If NSA was turned into an amusement park and the U.S. foreswore signals intelligence, not only would the world be more dangerous for us all, but foreign collection on Germany would not cease.

An accurate understanding of how and why the U.S. conducts its intelligence activities is essential for this enquiry. The U.S. has a highly formalized structure for oversight and approval that governs tasking and collection. Part of this structure involves an annual recalibration of the objectives of intelligence collection. Presidential decisions lay out the strategic priorities for collection. These collection priorities are now (and have been for years) counter-terrorism, counterintelligence, nonproliferation, and discerning the plans and capabilities of our likely military opponents. The 1981 Executive Order 12333, which has since been amended several times, codifies and constrains these intelligence priorities and activities. These four priorities consume the bulk of collection resources. A bureaucratic procedure takes the priorities developed in an interagency process led by the White House and translate them into specific actions and collection targets that then guide agency actions.

Signals intelligence is an important part of this collection and has dominated American intelligence collection for more than a decade. In part, this reflect the ease of collection that results from the vulnerability of internet technologies. It also reflects a certain lack of aptitude for human intelligence by the United States and the necessity of reallocating human intelligence resources to support the military conflicts in Iraq and Afghanistan. Signals intelligence compensates for this. It is best to think of the signals intelligence process as a pyramid with a massive base involving the trillions of messages transmitted each day and a small apex, where some thousands of these messages are sent to a human analyst for review. Only a fraction of all traffic is collected and only a tiny fraction of what is collected is read.

You already know that NSA's surveillance programs for counterterrorism were carried out in cooperation with more than thirty countries, including with Germany. The counter-terrorism objectives set for NSA reflect real security problems for the United States and its allies. The initial task is to look for patterns and connections among the collected traffic. A phone is captured in Syria. The list of contacts and calls on that phone provides objectives for further collection. If these connections suggest involvement in some activity of national security concern, the individual in question becomes the object of greater scrutiny. Most of this sorting and correlation is automated and out of every ten thousand messages perhaps only one is read. Of course, if an individual is linked to a collection priority, they will receive much greater attention. But for the average citizen not involved in terrorism, espionage, the proliferation of weapons of mass destruction, or hostile intelligence operations, the probability that NSA is reading their communications is nil.

The United States did not possess foreign intelligence agencies until the Second World War. NSA had a predecessor office created during World War One, but it was closed in the 1920s when the Secretary of State opined that “Gentlemen do not read other gentleman’s mail.” Franklin Roosevelt reversed this decision in the 1930s when confronted by the twin challenges of European fascism and Japanese imperialism.

At the end of World War II, the U.S., as in 1919, began to dismantle its foreign intelligence establishment, but President Truman changed this decision in response to the actions of Stalin and the Soviet Union. The National Security Act of 1947 created the structure and legal authorities for a global confrontation with Soviet totalitarianism. It authorized a civilian intelligence agency, the Central Intelligence Agency (CIA). President Truman also created the National Security Agency (NSA), which centralized the signals intelligence functions carried out in World War II by the military.

Confronted by the strategic challenge of assessing Soviet nuclear forces, the difficulty of operating human agents in the Soviet Bloc, and the Sputnik surprise, President Eisenhower fused CIA and Air Force space reconnaissance efforts into the National Reconnaissance Office. CIA, NSA are the principle foreign intelligence collection agencies and, with the Federal Bureau of Investigation (FBI), which is responsible for domestic intelligence activities, are the most important intelligence agencies. The National Geospatial-Intelligence Agency (NGA) is a relatively new agency that provides geospatial intelligence based on satellite imagery and other data sources. We could add the Defense Intelligence Agency to this list, but its activities and expertise are confined to military assessments.

One central element of the U.S. intelligence structure is an unparalleled degree of oversight by courts and Congress. The foreign intelligence establishment was created to serve the President in the exercise of his or her Constitutional responsibilities to defend the Republic in a global struggle to preserve democracy. Before 1970, these agencies, as is still the case in most other countries, were creatures of the President, with little or no oversight of their activities outside of the Executive Branch. In the 1970s, as part of larger social changes and in reaction to the unpopular wars in Southeast Asia and the misuse of intelligence agency assets for domestic political purposes by President Nixon, Congress imposed oversight legal constraints requirements on the intelligence community, constraining Presidential authority to undertake activities without consent from the legislative and judicial branches of government.

Few countries, including many European countries, can match this degree of oversight. The intent of oversight is to prevent the misuse of intelligence resources, to protect the civil liberties of Americans, and to ensure that intelligence activities match America’s strategic priorities. The setting of collection priorities by the White House is another element of this oversight – intelligence agencies do not do whatever they want. It would be fair to say that this oversight system protects Americans much more than foreigners, but this is the norm around the world for intelligence activities.

It is always interesting to hear Europeans describe how oversight works in the U.S. because these descriptions are almost always wrong. Take, for example, the charge that the Foreign Intelligence Surveillance court is a rubber stamp. People look at the number of cases approved

and the number of cases rejected in the final step of the process, and do not count the number of cases that did not reach the court because they were first rejected by the lawyers of the submitting agency or then rejected by the Department of Justice as it reviews submission to the FISC. Nor does this count the number of cases sent back for revision or strengthening. To reach the FISC, cases go through multiple reviews and weaker cases never reach the court. You may complain that the American oversight system does a better job of protecting American citizens than it does in protecting foreigners, but this kind of discrepancy in treatment can be found in all democracies.

The 1976 Final Report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities led to the Foreign Intelligence Surveillance Act and the creation of Congressional oversight committees and a special court. Congress and the Courts have oversight responsibility for ensuring that U.S. agencies operate in a legal manner. The President also ensures that espionage is conducted in accordance with the law, but also has unique responsibilities to ensure that intelligence agencies are operating in ways that make political and strategic sense. To do this, he or she relies on the staff of the National Security Council. Success requires dynamic engagement and leadership and a clear sense of U.S. goals. It is the NSC that must weigh and recommend to the President when the political risks of espionage outweigh the benefits, but the President is also supported by key advisory boards composed of outside experts and former senior officials, the President's Intelligence Advisory Board and the Privacy and Civil Liberties Oversight Board. These groups are regularly briefed on U.S. intelligence activities and report their views to the President.

Before the reforms of the 1970s, the lack of transparency generated a degree of hysteria about intelligence that still colors popular conceptions of espionage, particularly as these inaccurate views have been warmly embraced by Hollywood to create an alternate universe. One of the reasons I entered government service in 1984 was to satisfy my curiosity about these ideas. In my brief time in government I worked with individuals at all levels in CIA, NSA and NRO. I never saw "rogue agents" or agencies. I never saw programs not authorized by the White House and not subjected to often intense legal scrutiny. U.S. intelligence agencies are giant bureaucracies with thousands of lawyers whose job is to ensure they abide by national and international law.

The most startling thing about U.S. espionage against Germany was the inadequacy of the strategic calculation of risk. The lesson is that the U.S. needs to rethink its reliance on signals intelligence and remake its partnership with a mature and powerful Germany. However, the U.S., like Germany, is having trouble adjusting to a new international environment where the roles of both nations had changed. The problem for this enquiry is not the legality of operations in Europe. Nor is the problem mass surveillance by NSA. The problem is the political decision to spy on European leaders. A case can be made that in some circumstances, this decision is correct. U.S. leaders may have failed to adequately consider these risks, but the objectives they set for NSA reflect real problems, not only terrorism, but also about proliferation-related activities and Russian political operations in Europe.

This enquiry could helpfully dismiss the notion that "friends don't spy on friends." If Germany did not spy on friends, it would be unique among nations. There is public information that not

spying on friends” does not accurately describe German behavior. For the U.S, this was no surprise nor a cause for great annoyance. It is expected. American counterintelligence reviews consistently show that major NATO allies have always been active in spying on the U.S. – not to the level of Russia or China, of course, but certainly enough to disqualify them from being considered for sainthood. American business executives or officials who visit European countries will routinely have their communications monitored and in some instances, their hotel rooms and luggage surreptitiously searched, something many Americans know from personal experience.

Let me give you a public example, published in the Wall Street Journal some years ago. The Director of Central Intelligence wrote in the mid-1990s, he travelled to Paris to warn that espionage against the U.S. was reaching intolerable levels and asked that it be reduced. His remarks, made ten years after the event, reflect the preferred way of managing such problems, discreetly and outside the glare of publicity. Frankly, this discreet is best, particularly among friends. Nor does the fact that the U.S. objected to French espionage reflect on the strength of the relationship. There is strong and close cooperation with France on key security issues. France is a valued partner and plays an irreplaceable role in the conflict with jihad and Daesh. We all support France, along with Germany and our other European allies in the difficult struggle against domestic terrorism and as you know, many, but not all, NSA activities were undertaken in partnership to support the battle with terrorist groups. I personally respect the French because if they say they will do something, they do it, which is not always the case with other nations. To be fair, the French could levy similar charges against the United States.

There are other less public examples that demonstrate that friends spy do indeed on friends. States have responsibilities to their citizens that require such actions. What this example shows is that relations among powerful states are complex and not explained by simple-minded platitudes drawn from family life. Many of our allies engage in some level of intelligence activity against us, but in no case are we (or they for our efforts) the primary focus for espionage. There is a degree of absurdity in this kind of spying, but given the nature of bureaucracy and politics, and the heavy burden of the responsibility for security that each government must shoulder, it is perhaps unavoidable.

In shouldering this burden, democracies must protect their citizens without compromising political freedoms. In democracies, citizens must be shielded from an over-powerful government, yet at the same time, citizens must be able to use government to defend their societies from a range of threats. Neither an absolute prohibition nor absolute license are the answer. It means finding a balance that lets government do things we would, in an ideal world, prefer not do but which are necessary in the world in which we actually live.

Ambivalence in German foreign policy over its new global role could lead to reasonable concerns in the U.S., and while espionage is not the best way to address these concerns, it also is a traditional tool used to inform diplomacy. Germany’s status and position in Europe and the world has changed. The United States needs a new kind of closer partnership with Germany to achieve its foreign policy goals for democratic governance and open markets. Both the United States and Germany would find it easier to achieve their foreign policy goals if they work

together, but this will require them to redefine national policies. Building this new partnership will not be easy or automatic.

As the world has come to depend on the internet, we need to rethink the rules that apply to it and make them robust enough to sustain our most important global infrastructure. International law does not touch espionage, keeping it as the reserve of sovereigns for their untrammelled action. There are very few international agreements constraining espionage. China's recent agreement to end commercial espionage is one. The 1942 agreement between the U.S. and UK is another, and that was made under very special circumstances. It may be time to consider additional formal agreements or understandings among friends that would establish boundaries and rules for communications intelligence. Any such measure, of course, would need to be reciprocal and ensure common levels of oversight among all democratic nations.

Rules on data protection could be an indirect way of approaching and regulating communications surveillance that avoids the problem that no sovereign will concede its ability to conduct espionage (and in many cases, even admit to it). Common understandings on data protection, their effect on security and innovation, and on oversight and transparency would help to regulate the conduct of espionage in a new technological environment, but these understanding must be based on reciprocity. The EU data protection rules, however, are inadequate as they do not apply to Europe's national intelligence agencies (whose actions fall outside the scope of Commission authorities). Moreover, the EU's strictures are not widely observed in other regions of the worlds. Finally, a doctrinaire and over-expansive defense of privacy will damage economic growth, innovation, and security.

In this regard, the recent agreement between the U.S. and the European Commission is disappointing from an American point of view, because of its complete lack of reciprocity and protections for American citizens. The U.S. agreed to provide protections for European citizens, but the Commission could not extend similar protection to Americans. The explanation that the data flows are only one way or that Commission does not have "competence" over intelligence issues, that this rests with the member states, and is in American eyes what we would call a "dodge" – essentially evading responsibility. The lack of reciprocity is deeply troubling, and arguing that U.S. citizen are covered by national protections is a facile and unpersuasive because there is direct experience that should American citizen are not protected at all.

The issue of reciprocity is essential if we are to discuss next step for a closer U.S -German intelligence relationship. These steps are in both countries' interest. We can build on an already strong relationship, one that will be tested anew by the domestic terrorism that Germany and other European nations face, and by Russian efforts to use covert action to weaken Europe, NATO and the U.S.

In all democracies, it is useful to consider ways to expand transparency and accountability, consistent with the State's obligation to protect its citizens. Strong oversight mechanisms and greater transparency are the keys to acceptance of intelligence programs and to credible accountability. While every nation must undertake some activities in secret, democracies requires that national priorities and policies are publicly discussed and that governments be accountable to their citizens. While each nations' parliamentary culture is different, there are

enough commonalities among democracies that best practices for oversight and transparency could be identified. While agreement on rules of espionage is unlikely, it would be possible to reach agreement on principles of national oversight and on principles to protect data both citizen and company data.

For me, this discussion is important in considering how we consider governance of the global information structure upon which we have all become dependent and which creates new vulnerabilities for democracy. Similarly, this discussion is important for adjusting the foreign policies of the West to a more volatile international environment where democracy is again challenged. In meeting this challenge, partnership between our two nations is essential for the defense of democracy and I hope that this Enquiry will strengthen it.

I thank you for this opportunity and will be happy to take any questions.