

Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON
FOREIGN CYBER THREATS TO THE UNITED STATES

Thursday, January 5, 2017

Washington, D.C.

ALDERSON COURT REPORTING
1155 CONNECTICUT AVENUE, N.W.

SUITE 200

WASHINGTON, D.C. 20036

(202) 289-2260

www.aldersonreporting.com

1 HEARING TO RECEIVE TESTIMONY ON
2 FOREIGN CYBER THREATS TO THE UNITED STATES

3
4 Thursday, January 5, 2017

5
6 U.S. Senate
7 Committee on Armed Services
8 Washington, D.C.
9

10 The committee met, pursuant to notice, at 9:29 a.m. in
11 Room SD-G50, Dirksen Senate Office Building, Hon. John McCain,
12 chairman of the committee, presiding.

13 Committee Members Present: Senators McCain, Inhofe,
14 Wicker, Fischer, Cotton, Rounds, Ernst, Tillis, Sullivan,
15 Graham, Cruz, Reed, Nelson, McCaskill, Shaheen, Gillibrand,
16 Blumenthal, Donnelly, Hirono, Kaine, King, and Heinrich.

17 Other Senators Present: Senators Purdue, Warren, Peters,
18 and Sasse.
19
20
21
22
23
24
25

1 OPENING STATEMENT OF HON. JOHN McCAIN, U.S. SENATOR FROM
2 ARIZONA

3 Chairman McCain: Well, good morning, everyone.

4 Before we begin, I want to welcome all our members back
5 to the committee and extend a special welcome to the new
6 members joining us. On the Republican side, we are joined by
7 Senator Purdue and Senator Sasse. On the Democrat side, we
8 are joined by Senator Warren and Senator Peters.

9 It is a special privilege to serve on this committee,
10 most of all because it affords us the opportunity to spend so
11 much time in the company of heroes, the men and women who
12 serve and sacrifice on our behalf every day. I hope you will
13 come to cherish your service on this committee as much as I
14 have over the years, and I look forward to working with each
15 of you.

16 The committee meets this morning for the first in a
17 series of hearings on cybersecurity to receive the testimony
18 on foreign cyber threats to the United States. I would like
19 to welcome our witnesses this morning: James Clapper,
20 Director of National Intelligence; Marcel Lettre, Under
21 Secretary of Defense for Intelligence; and Admiral Mike
22 Rogers, Commander of U.S. Cyber Command, Director of the
23 National Security Agency, and Chief of the Central Security
24 Service.

25 This hearing is about the range of cybersecurity

1 challenges confronting our Nation, threats from countries like
2 Russia, China, and North Korea and Iran, as well as non-state
3 actors from terrorist groups to transnational criminal
4 organizations. In recent years, we have seen a growing series
5 of cyber attacks by multiple actors, attacks that have
6 targeted our citizens, businesses, military, and government.
7 But there is no escaping the fact that this committee meets
8 today for the first time in this new Congress in the aftermath
9 of an unprecedented attack on our democracy.

10 At the President's direction, Director Clapper is leading
11 a comprehensive review of Russian interference in our recent
12 election with the goal of informing the American people as
13 much as possible about what happened. I am confident that
14 Director Clapper will conduct this review with the same
15 integrity and professionalism that has characterized his
16 nearly half a century of government and military service. I
17 am equally confident in the dedicated members of our
18 intelligence community.

19 The goal of this review, as I understand it, is not to
20 question the outcome of the presidential election. Nor should
21 it be. As both President Obama and President-elect Trump have
22 said, our Nation must move forward. But we must do so with
23 full knowledge of the facts. I trust Director Clapper will
24 brief the Congress on his review when it is completed. This
25 is not the time or place to preview its findings.

1 That said, we know a lot already. In October, our
2 intelligence agencies concluded unanimously that, quote, the
3 Russian Government directed compromises of emails from U.S.
4 persons and institutions, including from U.S. political
5 organizations. They also assessed that, quote, disclosures of
6 alleged hacked emails were consistent with the methods and
7 motivations of Russian-directed efforts and that these thefts
8 and disclosures were intended to interfere with the U.S.
9 election process.

10 Since then, our intelligence community has released
11 additional information concerning these Russian activities,
12 including a joint analysis report that provided technical
13 details regarding the tools and infrastructure used by the
14 Russian civilian and military intelligence services to attack
15 the United States.

16 Every American should be alarmed by Russia's attacks on
17 our Nation. There is no national security interest more vital
18 to the United States of America than the ability to hold free
19 and fair elections without foreign interference. That is why
20 Congress must set partisanship aside, follow the facts, and
21 work together to devise comprehensive solutions to deter,
22 defend against and, when necessary, respond to foreign cyber
23 attacks.

24 As we do, we must recognize that the recent Russian
25 attacks are one part of a much bigger cyber problem. Russian

1 cyber attacks have targeted the White House, the Joint Staff,
2 the State Department, our critical infrastructure. Chinese
3 cyber attacks have reportedly targeted NASA, the Departments
4 of State and Commerce, congressional offices, military labs,
5 the Naval War College, and U.S. businesses, including major
6 defense contractors. Most recently, China compromised over 20
7 million background investigations at the Office of Personnel
8 Management. Iran has used cyber tools in recent years to
9 attack the U.S. Navy, U.S. partners in the Middle East, major
10 financial institutions, and a dam just 25 miles north of New
11 York City. And of course, North Korea was responsible for the
12 massive cyber attack on Sony Pictures in 2014.

13 What seems clear is that our adversaries have reached a
14 common conclusion: that the reward for attacking America in
15 cyberspace outweighs the risk. For years, cyber attacks on
16 our Nation have been met with indecision and inaction. Our
17 Nation has no policy and thus no strategy for cyber
18 deterrence. This appearance of weakness has been provocative
19 to our adversaries who have attacked us again and again with
20 growing severity. Unless we demonstrate that the costs of
21 attacking the United States outweigh the perceived benefits,
22 these cyber attacks will only grow.

23 This is also true beyond the cyber domain. It should not
24 surprise us that Vladimir Putin would think he could launch
25 increasingly severe cyber attacks against our Nation when he

1 has paid little price for invading Ukraine, annexing Crimea,
2 subverting democratic values and institutions across Europe,
3 and of course, helping Bashar Assad slaughter civilians in
4 Syria for more than a year with impunity. The same is true
5 for China, Iran, North Korea, and any other adversary that has
6 recently felt emboldened to challenge the world order. Put
7 simply, we cannot achieve cyber deterrence without restoring
8 the credibility of U.S. deterrence more broadly.

9 To do so, we must first have a policy, which means
10 finally resolving the long list of basic cyber questions that
11 we as a Nation have yet to answer. What constitutes an act of
12 war or aggression in cyberspace that would merit a military
13 response, be it by cyber or other means? What is our theory
14 of cyber deterrence, and what is our strategy to implement it?

15 Is our government organized appropriately to handle this
16 threat, or are we so stove-piped that we cannot deal with it
17 effectively? Who is accountable for this problem, and do they
18 have sufficient authorities to deliver results? Are we in the
19 Congress just as stove-piped on cyber as the executive branch
20 such that our oversight actually reinforces problems rather
21 than helping to resolve them? Do we need to change how we are
22 organized?

23 This committee intends to hold a series of hearings in
24 the months ahead to explore these and other questions. And we
25 look forward to hearing the candid views of our distinguished

1 witnesses today who have thought about and worked on these
2 questions as much as anyone in our Nation.

3 Senator Reed?

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 STATEMENT OF HON. JACK REED, U.S. SENATOR FROM RHODE
2 ISLAND

3 Senator Reed: Well, thank you very much, Mr. Chairman. I
4 want to commend you for your leadership in promptly scheduling
5 this hearing on foreign cyber threats.

6 I would also like to welcome our witnesses: Director
7 Clapper, Under Secretary Lettre, and Admiral Rogers. Thank
8 you, gentlemen, for your service and your dedication.

9 While I understand that our witnesses will be discussing
10 the cyber threats that many countries, including China and
11 India, pose to our Nation, I would like to focus for a few
12 minutes on the widely reported instances of Russian hacking
13 and disinformation that raised concerns regarding the election
14 of 2016.

15 In addition to stealing information from the Democratic
16 National Committee and the Clinton campaign and cherry-picking
17 what information it leaked to the media, the Russian
18 Government also created and spread fake news and conspiracies
19 across the vast social media landscape. At the very least,
20 the effect of Russia's actions was to erode the faith of the
21 American people in our democratic institutions. These and
22 other cyber tools remain highly active and engaged in
23 misinforming our political dialogue even today.

24 There is still much we do not know, but Russia's
25 involvement in these intrusions does not appear to be in any

1 doubt. Russia's best cyber operators are judged to be as
2 elusive and hard to identify as any in the world. In this
3 case, however, detection and attribution were not so
4 difficult, the implication being that Putin may have wanted us
5 to know what he had done, seeking only a level of plausible
6 deniability to support an official rejection of culpability.

7 These Russian cyber attacks should be judged within the
8 larger context of Russia's rejection of the post-Cold War
9 international order and aggressive actions against its
10 neighbors. Russia's current leaders, and President Putin in
11 particularly, perceive the democratic movements in the former
12 Soviet states, the West's general support for human rights,
13 press freedoms, the rule of law and democracy, as well as NATO
14 and EU enlargement, as a threat to what they believe is
15 Russia's sphere of influence.

16 Putin's Russia makes no secret of the fact that it is
17 determined to aggressively halt and counter what it
18 characterizes as Western encroachment on its vital interests.
19 The invasion of Georgia, the annexation of Crimea, the
20 aggression against Ukraine featuring sophisticated hybrid
21 warfare techniques, the continuing military buildup despite a
22 declining economy, saber-rattling in the Baltics and Baltic
23 Sea, the authoritarian onslaught against the press, NGOs, and
24 what remains of the Russian democratic opposition, the
25 unwavering campaign for national sovereignty over the

1 Internet, and the creation of an "iron information curtain"
2 like China's Great Firewall and its aggressive interference in
3 Western political processes all are of one piece. Russia's
4 efforts to undermine democracy at home and abroad and
5 destabilize the countries on its border cannot be ignored or
6 traded away in exchange for the appearance of comity.

7 Furthermore, what Russia did to the United States in
8 2016, it has already done and continues to do in Europe. This
9 challenge to the progress of democratic values since the end
10 of the Cold War must not be tolerated.

11 Despite the indifference of some to this matter, our
12 Nation needs to know in detail what the intelligence community
13 has concluded was an assault by senior officials of a foreign
14 government on our electoral process.

15 Our electoral process is the bedrock of our system of
16 government. An effort to manipulate it, especially by a
17 regime with values and interests so antithetical to our own,
18 is a challenge to the Nation's security which much be met with
19 bipartisan and universal condemnation, consequences, and
20 correction.

21 I believe the most appropriate means to conduct an
22 inquiry is the creation of a special select committee in the
23 Senate, since this issue and the solutions to the problems it
24 has exposed spill across the jurisdictional divides of the
25 standing committees on Armed Services, Intelligence, Foreign

1 Relations, Homeland Security, and Judiciary. Failing that,
2 our committee must take on as much of this task as we can, and
3 I again commend the chairman for his commitment to do so.

4 Therefore, I am pleased and grateful that his efforts
5 will be extended, the energy will be invested on the matters
6 that are so critical to the American people. I also want to
7 applaud President Obama's initial steps publicized last week
8 to respond to Russia's hostile actions.

9 General Clapper, Under Secretary Lettre, Admiral Rogers,
10 we appreciate your urgent efforts to discover what happened
11 and why and to make these facts known to the President, the
12 President-elect, Congress, and the American people. Although
13 your investigation and report to President Obama is not yet
14 public, we hope you will be able to convey and explain what
15 has been accomplished so far, including the steps already
16 announced by the President.

17 In addition, I am sure we will have many questions about
18 how we are organized in the cyber domain and what changes you
19 have recommended going forward, subjects that President Obama
20 referenced in his signing statement of the National Defense
21 Authorization Act for Fiscal Year 2017.

22 These are difficult issues, but they are of vital
23 importance to our Nation, our security, and our democracy.
24 Mr. Chairman, I look forward to working with you in a
25 bipartisan manner to conduct a thorough and thoughtful inquiry

1 and to do more to address the cyber threats our Nation faces
2 more broadly by state and non-state actors. Thank you very
3 much.

4 Chairman McCain: Welcome to the witnesses, and Mr.
5 Secretary, we will begin with you for any opening statements
6 or comment you might have.

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 STATEMENT OF HON. MARCEL J. LETTRE II, UNDER SECRETARY
2 OF DEFENSE FOR INTELLIGENCE

3 Mr. Lettre: Thank you, Chairman, Ranking Member Reed,
4 members of the committee. I appreciate the opportunity to be
5 here today. I will shortly turn the microphone over to
6 Director Clapper for some comments, followed by Admiral
7 Rogers. As this is my last appearance before this committee
8 before stepping down from 8 years of Pentagon service in a few
9 weeks, I want to --

10 Chairman McCain: I am sure you will regret not having
11 that opportunity again.

12 [Laughter.]

13 Mr. Lettre: It will be nice to be skiing a little bit in
14 February. That is for sure.

15 But having said that, since I am just a few weeks from
16 stepping down, I do want to thank this committee for its
17 partnership and I want to thank Director Clapper and admiral
18 Rogers for the privilege of being able to serve together with
19 them in the leadership of the U.S. intelligence community.
20 And to the men and women of the U.S. intelligence community,
21 civilian and military, thousands of whom are deployed today
22 around the world advancing U.S. interests and protecting
23 America, I do admire your integrity. I admire your service.
24 It has been an honor to serve with you over the last many
25 years.

1 In the interest of time, I will briefly note the
2 Department of Defense's views on cyber in three core themes:
3 first, the threats we must address; second, what we are doing
4 to address them now; and third, the difficult but urgent work
5 we know still lies ahead.

6 First, the threats. As you know, the Department of
7 Defense's leadership believes we confront no fewer than five
8 immediate but also distinct and evolving challenges across all
9 operating domains. We are countering the prospect of Russian
10 aggression and coercion, especially in Europe, something we
11 unfortunately we have had to energetically renew our focus on
12 in the last several years.

13 We are also managing historic change in perhaps the most
14 consequential region for America's future, the Asia-Pacific,
15 and watching for risks associated with China's destabilizing
16 actions in the region.

17 We are checking Iranian aggression and malign influence
18 across the Middle East.

19 We are strengthening our deterrent and defense forces in
20 the face of North Korea's continued nuclear and missile
21 provocations.

22 And we are countering terrorism with the aim of
23 accelerating the lasting defeat of ISIL and Al Qaeda.

24 These are what many in the Department of Defense have
25 termed the Four Plus One, four state-based challenges and an

1 ongoing condition of battling terrorism.

2 As our joint written statement for the record has
3 detailed, each of these security challenges, China, Russia,
4 Iran, North Korea, and global terrorist groups such as ISIL,
5 presents a significant cyber threat dimension to the U.S.
6 military. Cyber is an operating domain that is real, complex,
7 dynamic, contested, and must be addressed.

8 Second, what we are doing about it. The Department of
9 Defense has for several years pursued a comprehensive strategy
10 for maintaining the necessary strategic dominance in this
11 domain. Secretary of Defense Ash Carter has pressed for DOD
12 to change, to adapt, and to innovate not only to meet today's
13 challenges but also to ensure that we effectively defend
14 against cyber threats well into an uncertain future.

15 We have built and continue to build the means and methods
16 that will strengthen our relative position against each of
17 these dimensions of the cyber threat. The government cyber
18 policies, reflected in presidential policy directives and
19 executive orders, provide guidance on the absolute necessity
20 of a whole-of-government approach critical to protecting our
21 Nation.

22 The Department has developed, refined, and published its
23 cyber strategy which clearly lays out three key DOD cyber
24 missions: defending DOD networks, providing cyber options for
25 our military commanders, and when called upon by our Nation's

1 leaders, defending the Nation against cyber attacks of
2 significant consequence.

3 As the Director and Admiral Rogers will note, since 2009,
4 the Department has matured Cyber Command to ensure clear
5 command responsibility and authority and growing capabilities
6 essential to our unity of effort for cyber operations.

7 We also continue to mature our cyber mission forces which
8 this fall achieved initial operating capability, or IOC,
9 status. This force is providing military capability to
10 execute our three missions in cyberspace. We are building new
11 capabilities and new tools for the cyber mission force to use.

12 Third, what remains to be done. As much as we have done,
13 we recognize there is much more to do. Let me mention just a
14 couple of those most important tasks here.

15 First, we need to continue to develop and refine our
16 national cyber policy framework, which includes the evolution
17 of all dimensions of our deterrence posture: the ability to
18 deny the adversary's objectives, to impose costs, and to
19 ensure that we have a resilient infrastructure to execute a
20 multi-domain mission. This refinement in evolution in our
21 deterrent thinking and capability will further empower
22 decision-making at net speed.

23 Second, within the Department, Cyber Command has matured
24 and is doing more to protect the Nation and support global
25 operations than ever before, and we need to continue, in fact,

1 accelerate this maturation. Accordingly, the Secretary of
2 Defense supports the elevation of Cyber Command to a unified
3 combatant command and supports ending the dual hat arrangement
4 for the leadership of NSA and Cyber Command and doing so
5 through a deliberate conditions-based approach while
6 continuing to leverage the shared capabilities and synergies.

7 And finally, we must redouble our efforts to deepen
8 partnerships between government and the private sector and
9 between the U.S. Government and our allies. We must continue
10 to seek help from American industry, the source of much of the
11 world's greatest technology talent, in innovating to find
12 cyber defense solutions, build resiliency into our critical
13 infrastructure systems, and strengthen our deterrence. With
14 our international allies and partners, we must work together
15 to promote stability in cyberspace, universal recognition that
16 existing international law applies in cyberspace, and the
17 adoption of voluntary peacetime norms of responsible state
18 behavior.

19 Mr. Chairman, thanks. I look forward to your questions.
20 I will now pass the baton to Director Clapper. Thank you.

21
22
23
24
25

1 [The prepared statement of Director Clapper, Mr. Lettre,
2 and Admiral Rogers follows:]

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 Chairman McCain: General Clapper?
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 STATEMENT OF HON. JAMES R. CLAPPER, JR., DIRECTOR OF
2 NATIONAL INTELLIGENCE

3 Director Clapper: Chairman McCain, Ranking Member Reed,
4 and distinguished members of the committee, first thanks very
5 much for your opening statements. Obviously, we are here
6 today to talk about cyber threats that face our Nation, and I
7 will offer some brief valedictory recommendations and a few
8 parting observations. I certainly want to take note of and
9 thank the members of the committee who are engaged on this
10 issue and have spoken to it publicly.

11 I know there is a great interest in the issue of Russian
12 interference in our electoral process based on the many
13 classified briefings the intelligence community has already
14 provided on this topic to the Congress. Secretary of Homeland
15 Security Jeh Johnson and I have issued statements about it.
16 The joint analysis report that you alluded to publicly issued
17 by the Department of Homeland Security and the Federal Bureau
18 of Investigation provided details on the tools and
19 infrastructure used by the Russian intelligence services to
20 compromise infrastructure associated with the election, as
21 well as a range of U.S. Government political and private
22 sector entities, as you described.

23 As you also noted, the President tasked the intelligence
24 community to prepare a comprehensive report on Russian
25 interference in our election. We plan to brief the Congress

1 and release an unclassified version of this report to the
2 public early next week with due deference to the protection of
3 highly sensitive and fragile sources and methods. But until
4 then, we are really not prepared to discuss this beyond
5 standing by our earlier statements. We are prepared to talk
6 about other aspects of the Russian cyber threat.

7 We also see cyber threats challenging public trust and
8 confidence in information services and institutions. Russia
9 has clearly assumed an even more aggressive cyber posture by
10 increasing cyber espionage operations, leaking data stolen
11 from these operations, and targeting critical infrastructure
12 systems.

13 China continues to succeed in conducting cyber espionage
14 against the U.S. Government, our allies, and U.S. companies.
15 The intelligence community and the security experts, however,
16 have observed some reduction in cyber activities from China
17 against U.S. companies since the bilateral September 2015
18 commitment to refrain from espionage for commercial gain.

19 Iran and North Korea continue to improve their
20 capabilities to launch disruptive or destructive cyber attacks
21 to support their political objectives.

22 Non-state actors, notably terrorist groups most
23 especially including ISIL, also continue to use the Internet
24 to organize, recruit, spread propaganda, raise funds, collect
25 intelligence, inspire action by disciples, and coordinate

1 operations. So in this regard, I want to foot stomp a few
2 points that I have made here before.

3 Rapidly advancing commercial encryption capabilities have
4 had profound effects on our ability to detect terrorists and
5 their activities. We need to strengthen the partnership
6 between government and industry and find the right balance to
7 enable the intelligence community and law enforcement both to
8 operate, as well as to continue to respect the rights to
9 privacy.

10 Cyber operations can also be a means to change,
11 manipulate, or falsify electronic data or information to
12 compromise its integrity. Cyberspace can be an echo chamber
13 in which information, ideas, or beliefs, true or false, get
14 amplified or reinforced through constant repetition. All
15 these types of cyber operations have the power to chip away at
16 public trust and confidence in our information, services, and
17 institutions.

18 By way of some observations and recommendations, both the
19 government and the private sector have done a lot to improve
20 cybersecurity, and our collective security is better but it is
21 still not good enough. Our Federal partners are stepping up
22 their efforts with the private sector but sharing what they
23 have remains uneven. I think the private sector needs to up
24 its game on cybersecurity and not just wait for the government
25 to provide perfect warning or a magic solution.

1 We need to influence international behavior in
2 cyberspace. This means pursuing more global diplomatic
3 efforts to promulgate norms of behavior in peacetime and to
4 explore setting limits on cyber operations against certain
5 targets.

6 When something major happens in cyberspace, our automatic
7 default policy position should not be exclusively to counter
8 cyber with cyber. We should consider all instruments of
9 national power. In most cases to date, non-cyber tools have
10 been more effective at changing our adversaries' cyber
11 behavior. When we do choose to act, we need to model the
12 rules we want others to follow since our actions set
13 precedents.

14 We also need to be prepared for adversary retaliation,
15 which may not be as surgical, either due to our adversary's
16 skill or the inherent difficulty in calibrating effect and
17 impact of cyber tools. That is why using cyber to counter
18 cyber attacks risks unintended consequences.

19 We currently cannot put a lot of stock, at least in my
20 mind, in cyber deterrence. Unlike nuclear weapons, cyber
21 capabilities are difficult to see and evaluate and are
22 ephemeral. It is accordingly very hard to create the
23 substance and psychology of deterrence in my view.

24 We also have to take some steps now to invest in the
25 future. We need to rebuild trusted working relationships with

1 industry and the private sector on specific issues like
2 encryption and the roles and responsibilities for government,
3 users, and industry.

4 I believe we need to separate NSA and CYBERCOM. We
5 should discontinue the temporary dual hat arrangement, which I
6 helped design when I was Under Secretary of Defense for
7 Intelligence 7 years ago. This is not purely a military
8 issue. I do not believe it is in the NSA's or the IC's long-
9 term best interest to continue the dual hat setup.

10 Third, we must hire, train, and retain enough cyber
11 talent and appropriately fuse cyber as a whole-of-IC
12 workforce. Clearly cyber will be a challenge for the U.S.,
13 the intelligence community, and our national security for the
14 foreseeable future, and we need to be prepared for that.
15 Adversaries are pushing the envelope since this is a tool that
16 does not cost much and sometimes is hard to attribute.

17 I certainly appreciate, as we all do, the committee's
18 interest in this difficult and important challenge.

19 I will wrap up by saying after 53 years in the
20 intelligence business in one capacity or another, happily I
21 have just got 15 days left.

22 [Laughter.]

23 Director Clapper: I will miss being involved in the
24 intelligence mission, and I will certainly miss the talented
25 and dedicated patriots who are in the United States

1 intelligence community. I am very proud of the community of
2 professionals I have represented here for the last 6 and a
3 half years who do not get much public recognition and who like
4 it that way. They have always supported me and I am confident
5 they will do no less for my successor, whoever that turns out
6 to be.

7 With that, let me stop and pass to Admiral Rogers.

8 Chairman McCain: Thank you, General.

9 Admiral Rogers?

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 STATEMENT OF ADMIRAL MICHAEL S. ROGERS, USN, COMMANDER,
2 UNITED STATES CYBER COMMAND; DIRECTOR, NATIONAL SECURITY
3 AGENCY; CHIEF, CENTRAL SECURITY SERVICES

4 Admiral Rogers: Chairman McCain, Ranking Member Reed,
5 members of the committee, good morning and thank you for the
6 opportunity to appear before the committee today on behalf of
7 the United States Cyber Command and the National Security
8 Agency.

9 I am honored to appear beside Director Clapper and Under
10 Secretary Lettre and I applaud them both for their many years
11 of public service. It has been a true honor, gentlemen.

12 When we last met in September, I discussed the changing
13 cyber threat environment, and today I look forward to further
14 discussing this complex issue. Of course, some aspects of
15 what we do must remain classified to protect our Nation's
16 security. So today I will limit my discussion to those in the
17 public domain.

18 We have seen over the course of the last year how this
19 cyber threat environment is constantly evolving. We have all
20 come to take for granted the interconnectivity that is being
21 built into every facet of our lives. It creates opportunities
22 and vulnerabilities. Those who would seek to harm our fellow
23 Americans and our Nation utilize the same Internet, the same
24 communications devices, and the same social media platforms
25 that we, our families and our friends here and around the

1 world use. We must keep pace with such changes in order to
2 provide policymakers and our operational commanders the
3 intelligence and cyber capabilities they need to keep us safe.
4 That means understanding our adversaries to the best of our
5 ability and understanding what they mean to do and why. We
6 are watching sophisticated adversaries involved in criminal
7 behavior, terrorism planning, malicious cyber activities, and
8 even outright cyber attacks. While this is a global problem,
9 we have also recently witnessed the use of these tactics here
10 at home.

11 The statement for the record that we have provided
12 jointly to this committee covers the threat picture worldwide,
13 but I know this hearing today will inevitably focus on reports
14 of interference in our recent elections. I echo Director
15 Clapper in saying that we will await the findings of the just-
16 completed intelligence review ordered by the President and
17 defer our comments on its specifics until after that review is
18 shared with our leaders and congressional overseers.

19 I do want to add, however, that over this last year, NSA
20 and Cyber Command have worked extensively with our broader
21 government partners to detect and monitor Russian cyber
22 activity. The hacking of organizations and systems belonging
23 to our election process is of great concern, and we will
24 continue to focus strongly on this activity.

25 For NSA's part, we focus on the foreign threat actor in

1 foreign spaces, but we share our information as readily as
2 possible with the rest of our partners in the Department of
3 Defense, the intelligence community, and Federal law
4 enforcement, as well as others within the U.S. Government and
5 the private sector.

6 As you know, Russian cyber groups have a history of
7 aggressively hacking into other countries' government
8 infrastructure and even election systems. And as I have
9 indicated, this will remain a top priority for NSA and U.S.
10 Cyber Command.

11 In this changing threat environment, I would like to take
12 this opportunity to emphasize the importance of improving
13 cybersecurity and working related issues across public and
14 private sectors. We continue to engage with our partners
15 around the world on what is acceptable and unacceptable
16 behavior in cyberspace, and we clearly are not where we want
17 to be, nor where we need to be in this regard.

18 We continue to make investments in technologies and
19 capabilities to improve detection of malicious cyber
20 activities and make it more difficult for malicious cyber
21 actors intending to do us harm. Combating cyber threats take
22 more than technology. It takes talented, motivated people,
23 and we are investing more than ever in the recruitment and
24 retention of a skilled workforce that is knowledgeable,
25 passionate, and dedicated to protecting the Nation for the

1 safety of our citizens and of our friends and allies around
2 the world.

3 Innovation is one of the key tenets of NSA and Cyber
4 Command and we need to invigorate the cyber workforce that
5 think creatively about challenges that do not ascribe to
6 traditional understandings of borders and boundaries. This
7 remains a key driver and a key challenge as we look to the
8 future.

9 Cyber Command is well along in building our cyber mission
10 force, deploying teams to defend the vital networks that
11 support DOD operations, to support combatant commanders in
12 their missions worldwide, and to bolster DOD's capacity and
13 capabilities to defend the Nation against cyber attacks of
14 significant consequence.

15 The organizations I lead, the U.S. Cyber Command and the
16 National Security Agency, have provided intelligence, expert
17 advice, and tailored options to the Nation's decision-makers
18 in response to recent events. Much of their activity can only
19 be discussed in classified channels, but I must say I am proud
20 of what both organizations have accomplished and will
21 accomplish, even as we acknowledge we have to do more.

22 I look forward to your questions.

23 And finally, on one personal note, I apologize to all of
24 you. I have an ongoing back issue, and if I have to stand up
25 in the course of this time period, please do not take that as

1 a sign of disrespect in any way. I guess I am just getting
2 older.

3 That is all I have for you, sir.

4 Chairman McCain: I know how you feel.

5 [Laughter.]

6 Chairman McCain: Director, I just have to -- General
7 Clapper, I just have to mention the name, Mr. Assange, has
8 popped up, and I believe that he is the one who is responsible
9 for publishing names of individuals that work for us that put
10 their lives in direct danger. Is that correct?

11 Director Clapper: Yes, he has.

12 Chairman McCain: And do you think that there is any
13 credibility we should attach to this individual given his
14 record of --

15 Director Clapper: Not in my view.

16 Chairman McCain: Not in your view.

17 Admiral Rogers?

18 Admiral Rogers: I second those comments.

19 Chairman McCain: Thank you.

20 For the record, on October 7th, the Homeland Security and
21 Office of the Director of National Intelligence -- their
22 assessment was that the U.S. intelligence community is
23 confident that the Russian Government directed the recent
24 compromise of emails from U.S. persons and institutions,
25 including from U.S. political organizations. It goes on to

1 say these thefts and disclosures are intended to interfere
2 with the U.S. election process. Quote, such activity is not
3 new to Moscow. Russians have used similar tactics and
4 techniques across Europe and Eurasia. Quote, based on the
5 scope and sensitivity of these efforts, only Russia's senior
6 most officials could have authorized these activities.

7 General Clapper, those are still operable and correct
8 statements?

9 Director Clapper: Yes, Chairman McCain, they are. As I
10 indicated in my statement, we stand actually more resolutely
11 on the strength of that statement that we made on the 7th of
12 October.

13 Chairman McCain: I thank you.

14 And so really what we are talking about is if they
15 succeeded in changing the results of an election, which none
16 of us believe they were, that would have to constitute an
17 attack on the United States of America because of the effects
18 if they had succeeded. Would you agree with that?

19 Director Clapper: First, we cannot say -- they did not
20 change any vote tallies or anything of that sort. We had no
21 way of gauging the impact that -- certainly the intelligence
22 community cannot gauge the impact it had on choices the
23 electorate made. There is no way for us to gauge that.

24 Whether or not that constitutes an act of war I think is
25 a very heavy policy call that I do not believe the

1 intelligence community should make. But it certainly would
2 carry in my view great gravity.

3 Chairman McCain: Thank you.

4 Admiral Rogers, have you seen this problem in your
5 position getting worse or better? In other words, it is my
6 information that their techniques have improved, their
7 capabilities improved. The degree of success has improved. Is
8 that your assessment?

9 Admiral Rogers: I have publicly said before that the
10 Russians are a peer competitor in cyber. If you look broadly
11 beyond the Russians to cyber at large, the level of capability
12 of nation states and actors around the world continues to
13 increase. I cannot think of a single significant actor out
14 there who is either decreasing their level of investment,
15 getting worse in their tradecraft or capability, or in any way
16 backing away from significant investments in cyber.

17 Chairman McCain: And with all due respect to you, Mr.
18 Secretary, I have not seen a policy. In other words, I do not
19 think any of our intelligence people know what to do if there
20 is an attack besides report it. I do not think that any of
21 our people know, if they see an attack coming, what specific
22 actions should be taken. Maybe I am missing something, but I
23 have asked time after time, what do you do in the case of an
24 attack? And there has not been an answer. There has not been
25 an answer. I believe that unless we have specific

1 instructions to these wonderful men and women who are doing
2 all this work, then we are going to be bystanders and
3 observers. I am glad to hear you respond to that.

4 Mr. Lettre: Mr. Chairman, you are right that we have a
5 lot more work to do to put the right deterrence and response
6 framework in place on cyber. This is somewhat of a new domain
7 of operations and in some cases warfare. And in my personal
8 opinion, the next administration would be well served to focus
9 very early on those questions of continuing to develop our
10 overarching policy, a comprehensive approach, and an
11 increasingly robust and refined deterrence framework.

12 Chairman McCain: I thank you.

13 Finally, Director and Admiral, would it make your job
14 easier if you did not have to report to seven different
15 committees?

16 Director Clapper: Chairman McCain, my hands have been
17 slapped before when I ventured into the delicate area of
18 congressional jurisdiction. In the remaining 15 days that I
19 am in office, I do not think I am going to speak to that.
20 Afterwards that might be different.

21 Chairman McCain: Well, we will look forward to calling
22 you back.

23 [Laughter.]

24 Chairman McCain: Admiral Rogers?

25 Admiral Rogers: Can I second the comments of the

1 Director of National Intelligence?

2 Chairman McCain: But it does make it difficult, does it
3 not? It is not exactly stove-piping, but overlapping
4 jurisdictions I think makes your job a little harder, does it
5 not, I mean in all candor, Admiral?

6 Admiral Rogers: The way I would phrase is I think
7 clearly an integrated approach is a key component of our
8 ability to move ahead here. I would say that in the
9 government, in the private sector, there is no particular one
10 slice where that is not applicable.

11 Chairman McCain: Thank you.

12 Senator Reed?

13 Senator Reed: Well, thank you very much, Mr. Chairman.

14 General Clapper, you responded to the chairman that in
15 October you and the Director of Homeland Security concluded
16 that the Russian Government intervened in the election. And
17 Admiral Rogers also seconded that view. That is also today
18 the view, for the record, of the FBI and the Central
19 Intelligence Agency, in fact, all the intelligence community.
20 Is that correct?

21 Director Clapper: Yes. The forthcoming report is done
22 essentially by those three agencies, CIA, FBI, and NSA.

23 Senator Reed: And the same conclusion with respect to
24 the involvement of high-level Russian authorities is shared by
25 all these agencies?

1 Director Clapper: Yes.

2 Senator Reed: The chairman just noticed the legislative
3 compartmentalization. Is that reflected also in terms of
4 operations, in terms of, for example, Admiral Rogers, if you
5 through NSA or through your sources detect something that is
6 obviously a disruption, something that is patently wrong, you
7 can communicate to the FBI or law enforcement, but there is no
8 mechanism to make things happen administratively. Is that
9 fair?

10 Admiral Rogers: There is certainly a process, and in
11 fact, there have been several instances that I can think of in
12 the last 18 months where we have run through that exact same
13 scenario. Intelligence, as it does in many other areas, other
14 domains, will detect incoming activity of concern. We, NSA,
15 will partner with FBI, the Department of Homeland Security,
16 U.S. Cyber Command to ensure the broader government, the
17 Department of Defense and FBI in its relationship with the
18 private sector.

19 But the biggest frustration to me is speed, speed, speed.
20 We have got to get faster. We have got to be more agile. And
21 so for me at least within my span of control, I am constantly
22 asking the team what can we do to be faster and more agile.
23 How do we organize ourselves? What is the construct that
24 makes the most sense? We cannot be bound by history and
25 tradition here, so to speak. We have to be willing to look at

1 alternatives.

2 Senator Reed: Thank you.

3 General Clapper, one of the aspects of this Russian
4 hacking was not just disseminating information that they had
5 exploited from computers, but also the allegations of fake
6 news sites, fake news stories that were propagated. Is that
7 accurate, or is that one aspect of this problem?

8 Director Clapper: Yes. Without getting too far in front
9 of the headlights of our rollout next week to the Congress,
10 this was a multifaceted campaign. So the hacking was only one
11 part of it, and it also entailed classical propaganda,
12 disinformation, fake news.

13 Senator Reed: Does that continue?

14 Director Clapper: Yes.

15 Senator Reed: The Russians particularly are very astute
16 at covering up their tracks. It appears that they were not
17 quite as diligent or -- let me ask a question.

18 Do you believe that they made little attempts to cover up
19 what they were doing as a way to make a point politically?

20 Director Clapper: Well, again, without preempting the
21 report, that is classical tradecraft that the Russians have
22 long used. Particularly when they are promulgating so-called
23 disinformation, they will often try to hide the source of that
24 or mask it to deliberately mask the source.

25 Senator Reed: Let me just ask one more time. In this

1 situation, though, were there attempts to mask their
2 involvement, very elaborate and very, very sophisticated, or
3 was it just enough to have plausible deniability?

4 Director Clapper: Sir, I would rather not get into that.
5 That kind of edges into the sources and methods and I would
6 rather not speak to that publicly.

7 Senator Reed: Fair enough.

8 These activities are ongoing now in Europe as Europe
9 prepares for elections. Is that a fair assumption?

10 Director Clapper: It is.

11 Senator Reed: Thank you.

12 Yesterday, the "Wall Street Journal" indicated that the
13 President-elect is considering changes to the intelligence
14 community. Have you at all, as the experts in this field,
15 been engaged in any of these discussions, deliberations,
16 advice?

17 Director Clapper: No, we have not.

18 Senator Reed: Thank you, Mr. Chairman.

19 Chairman McCain: Senator Inhofe?

20 Senator Inhofe: Thank you, Mr. Chairman.

21 I heard this morning that a lot of the news media was
22 characterizing this as a hearing on Russian hacking, and
23 actually it is on foreign cyber threats to the United States.
24 I am trying to cover a couple of the other ones.

25 First of all, I received something this morning, Director

1 Clapper, that I was very glad to read. I have often said that
2 the threats we are facing today are greater. I look wistfully
3 back at the days of the Cold War. Your statement that was in
4 print this morning said sometimes all of this makes me long
5 for the Cold War when the world essentially had two large
6 mutually exclusive -- and so forth.

7 You know, I think it is important that we talk about this
8 because the general public is not aware of the nature of the
9 threats that are out there that have not been out there
10 before.

11 Admiral -- no. Director Clapper, we have had a lot of
12 most damaging cyber attacks perpetrated against the American
13 people. When the chairman gave his opening statement, he
14 singled out three or four of them. One of them was the OPM
15 incident. That was 2014 and 2015, Office of Personnel
16 Management. It was a breach and threat to personal
17 information, birthdates, home addresses, Social Security
18 numbers of over 22 million individuals.

19 I would like to ask you what action was taken after that
20 and what kind of effect that might have had on the behavior of
21 the Chinese.

22 Director Clapper: Well, the major action that we took,
23 of course, was remediation in terms of advising people of what
24 the potential risks were. And, of course, there was a lot of
25 work done. NSA was deeply involved in this in enhancing or

1 improving the cybersecurity posture of OPM, and Admiral Rogers
2 might speak to that.

3 I would say that this was espionage. It was not an
4 attack per se. And, of course, I am always a bit reticent
5 about people who live in glass houses should not throw
6 publicly too many rocks. So there is I think a difference
7 between an act of espionage, which we conduct as well and
8 other nations do, versus an attack.

9 Mike, do you want to comment?

10 Admiral Rogers: Just as a broader point, I think the OPM
11 issue highlights that massive data concentrations increasingly
12 have value all of their own. What do I mean by that? I can
13 remember 10 years ago earlier in my time in cyber thinking to
14 myself large databases like OPM are so large. The ability of
15 an intruder, an external actor to actually access, fully
16 extract, and bore their way through millions upon millions of
17 records would be difficult. But with the power of big data
18 analytics, large data concentrations now become increasingly
19 attractive targets because the ability to mine that data for
20 insights, which is what we think drove this action in the
21 first place, becomes more and more easily done.

22 Senator Inhofe: Okay. I appreciate that very much.

23 In your joint statement -- by the way, I like the idea of
24 joint statements. It makes our questioning a lot easier.

25 You talk about the -- you end up stating through one of

1 your paragraphs, in short, cyber threat cannot be eliminated.

2 Rather, cyber threat must be managed. And it is interesting
3 that in the Edison Electric Institute -- it is a publication.
4 I think it just came in this morning -- they say exactly the
5 same thing. This seems to be one of the rare cases where we
6 have government and industry working together. Their
7 statement was the electric power industry recognizes it cannot
8 protect all assets from all threats and instead must manage
9 risk.

10 Now, they go on to describe working together with
11 government, and they say the industry's security strategy is
12 constantly evolved and are closely coordinated with the
13 Federal Government through a partnership called the
14 Electricity Subsector Coordinating Council, ESCC. Can you
15 comment? Are we looking at getting some success out of that?

16 Director Clapper: I think it is emblematic of a lot of
17 work that the intelligence community has done, the Department
18 of Homeland Security in engaging with each of the, I think, 16
19 key infrastructure sectors in this country and providing --
20 what we have embarked on is providing them, tailored to each
21 one of those sectors, intelligence estimates of what the
22 threats and vulnerabilities are in order to help them take
23 measures to enhance their cybersecurity.

24 I think the major point here is that if there is any
25 connection whatsoever with the Internet, there is an inherent

1 security vulnerability, and we have to manage the risk that is
2 generated accordingly with full knowledge of that fact. If
3 there is an Internet connection, there is always going to be a
4 vulnerability.

5 Mike?

6 Admiral Rogers: I would echo that. I think part of our
7 challenge is our defensive strategy must be two-pronged. We
8 have to spend time making it difficult for people to gain
9 access, but we must acknowledge that despite our best efforts,
10 there is a probability that they are still going to get in.

11 So what do you do? As a guy who defends networks on the
12 Cyber Command side, I would tell you it is a whole different
13 process, methodology, prioritization, and risk approach in
14 dealing with someone who is already in your network versus
15 trying to keep them out in the first place. And we have to do
16 both.

17 Senator Inhofe: I appreciate that. My time has expired.
18 I have one last question just for the record. You cannot
19 answer it at this time.

20 But a year ago -- it is a year and 2 months ago I think
21 it was, Admiral Rogers -- you made the statement before this
22 committee that, quote, we have peer competitors in cyberspace
23 and some of them have already hinted that they hold the power
24 to cripple our infrastructure and set back our standard of
25 living if they choose. I would like for the record if you

1 could just kind of outline which of our peer competitors might
2 be the closest to choosing to use their power.

3 Admiral Rogers: As I have publicly said before, the
4 Russians are the peer competitor to us. But I look at other
5 nations. You look at China, for example, and the level of
6 capability and investment they are making. I am watching
7 their abilities rise significantly. Iran, North Korea,
8 currently at a moderate level. But clearly the level of
9 investment, the capability we are seeing, and their
10 willingness to employ cyber in some very aggressive ways that
11 would be way beyond our normal risk calculus is of concern.

12 Senator Inhofe: Thank you, Mr. Chairman.

13 Chairman McCain: Senator Nelson?

14 Senator Nelson: I think it is the general assumption
15 that you all have said that our systems can be invaded that
16 has the American people, we as policymakers concerned, but the
17 average American concerned that there is no privacy anymore.

18 General, do you think in the report next week that you
19 all will ascribe a motivation to Putin for the election
20 attempt?

21 Director Clapper: Yes, we will ascribe a motivation. I
22 would rather not, again, preempt the report.

23 Senator Nelson: Understood.

24 Well, then will you discuss after the report what is
25 sufficient in the future to impose enough cost to make them

1 stop this kind of activity?

2 Director Clapper: No. If we are going to speak to that,
3 that would be separate from the report. What the report will
4 include, per the President's tasking, was a section
5 contributed by the Department of Homeland Security and NIST, I
6 believe, on best practices for defending, but it does not
7 speak to that, which is really out of our lane. That is a
8 policy call.

9 Senator Nelson: So we are now talking about deterrence,
10 and as one of you said in your testimony, it is not like the
11 nuclear standoff of mutually assured destruction because we do
12 not have a particular deterrence now. Would you discuss that?

13 Director Clapper: The point I was trying to make is that
14 in the case of nuclear deterrence, there are instruments you
15 can see, feel, touch, measure, weaponry. We have had a
16 demonstration a long time ago of the impact of nuclear
17 weaponry. And that is what creates both the physical
18 substance of deterrence, as well as the psychology. And the
19 problem with the cyber domain -- it does not have those
20 physical dimensions that you can measure, see, feel, and touch
21 as we do with nuclear deterrence.

22 Senator Nelson: So let me give you an example. Help us
23 understand had the supposed invasion into the Vermont utility
24 been in fact an invasion by a foreign power and ascribed to
25 that was shutting it down, if that had been the case, what

1 would be some of the options we would do.

2 Director Clapper: Well, again, this would be a -- as I
3 understand it, by the way, it was not. But had it been from
4 the malware planted by a foreign power, I think that is
5 something that would be very situational dependent as to what
6 to do about it. As I indicated in my remarks, perhaps a cyber
7 reaction to a cyber act may not be the best course of action.
8 Some other form of national power. Sanctions is what we have
9 traditionally used.

10 And as I also indicated, the problem, at least for me,
11 is-- and I will ask others to speak if they want to -- if you
12 do retaliate in a cyber context, not knowing exactly what
13 counter-retaliation you will get back. We go through all
14 kinds of exquisite thought processes on deciding how to react.

15 We try to be very surgical, very precise. We try to gauge
16 what the second order or unintended consequences might be. I
17 do not think others are similarly disposed to consider such
18 precision and such exactness when they respond. So there is
19 always that issue of counter-retaliation, ergo my brief
20 mention that it is in my view best to consider all instruments
21 of national power.

22 Senator Nelson: And I think that is what is concerning
23 us. Could we, the United States -- do we have the ability
24 that we could make it so tough on North Korea with a cyber
25 attack that it would deter them from some of their strange

1 behavior?

2 Director Clapper: Not necessarily via a direct cyber
3 reaction, given the difficulty of gaining access to their
4 cyber networks.

5 Chairman McCain: Senator Wicker?

6 Senator Wicker: Thank you.

7 Director Clapper, you are pretty far along on the report
8 that will be released next week, obviously. How far along are
9 you? And what do you lack and how will this be released?
10 Will it be in a classified format? Will you be willing to
11 testify in an opening hearing like this, or will we need to go
12 down the SCIF to hear this?

13 Director Clapper: What is planned is a series of
14 briefings in the Congress. I think I have four more hearings
15 to do, first with our oversight committees, which will be
16 closed hearings I believe. And then there will be all-House,
17 all-Senate hearings I believe next week as we roll out a
18 version of the report --

19 Senator Wicker: So those will be classified.

20 Director Clapper: -- followed by an unclassified
21 version.

22 Senator Wicker: I see. So the public will not hear
23 sources and methods, but you think it will be fairly
24 convincing without going beyond what --

25 Director Clapper: I assure you that I intend to push the

1 envelope as much as I can particularly on the unclassified
2 version because I think the public should know as much about
3 this as possible. This is why I felt very strongly about the
4 statement we made in October. And so we will be as
5 forthcoming as we can, but there are some sensitive and
6 fragile sources and methods here, which is one reason why we
7 are reticent to talk about it in this setting.

8 Senator Wicker: And you have said that, and I expect you
9 will be challenged with some very talented questioners up and
10 down the dais here today on that.

11 I would have to support what Senator Nelson has said. As
12 regrettable and reprehensible as the hacking of political
13 parties is, I do think Senator Nelson has touched on really
14 the larger issue which really is the subject matter of this
15 hearing and that is what the real threats are. And it
16 concerns me that we really do not know what the deterrence
17 ought to be. And I wonder at what level are conversations
18 taking place within the administration or within the
19 intelligence community about what is appropriate in terms of a
20 response. You mentioned countering cyber with cyber is not
21 necessarily the number one solution. Secretary Lettre
22 mentioned that we should impose costs, and perhaps after you
23 answer, I can ask him to expound on that also.

24 Director Clapper: Well, we have had many discussions in
25 the White House situation room at Deputies Committee,

1 Principals Committee, and NSC meetings about what to do when
2 we have these attacks. I think the Sony attack by the North
3 Koreans is a case in point. And there you get into the
4 complexities of if you launch a counter cyber attack -- I want
5 to be careful here, but you have to use some other nation's
6 infrastructure in order to mount that attack. That gets into,
7 as I have learned, complex legal issues involving
8 international law. And so the judgment was to impose some
9 other costs other than a direct cyber retaliation.

10 Senator Wicker: Did you recommend the President's
11 sanctions? Were his actions in response to the Russian
12 hacking part of your recommendation, or did that come from
13 someone else?

14 Director Clapper: Well, without going into internal
15 decision-making, I think that was a consensus interagency
16 view.

17 Senator Wicker: Secretary Lettre, what about imposing
18 costs? What did you mean by that?

19 Mr. Lettre: Well, as part of an approach to deterrence
20 that takes each case as it comes up case by case, we need to
21 look at ways to respond -- first deter and then respond to
22 attacks at a time and a place of our choosing that favors
23 advantages that we have as we use all of the instruments
24 available. So we look to deny objectives and then impose
25 costs, as you indicated, Senator.

1 Imposing costs really can come from things like were
2 announced last week with the sanctions that were applied in
3 the case of the Russian hacking situation, but they can go
4 more broadly than that. From the military's perspective, we
5 are concerned not just about Russia's cyber hacking, but also
6 about a range of aggressive actions by Russia across multiple
7 regions of the globe. And so we look to impose costs on
8 Russia by a range of measures across multiple regions in
9 partnership with our allies through NATO, where we can, to
10 push back on Russian actions and deter future aggressive
11 actions. So that is a bit of what we mean by imposing costs
12 here.

13 Senator Wicker: Thank you.

14 Chairman McCain: It seems that every attack is handled
15 on a case-by-case basis, and that is not a strategy.

16 Senator McCaskill?

17 Senator McCaskill: Thank you.

18 I know this will probably confuse you a little bit,
19 General Clapper, but review again how long you have been
20 working in intelligence.

21 Director Clapper: I started in 1963.

22 Senator McCaskill: And you enlisted in 1963. Correct?

23 Director Clapper: No. I enlisted in the Marine Corps in
24 1961.

25 Senator McCaskill: And then transferred to the Air

1 Force?

2 Director Clapper: Right.

3 Senator McCaskill: And you flew support for combat
4 missions in Vietnam?

5 Director Clapper: I did two tours in Southeast Asia, one
6 in Vietnam in 1965 and 1966, and then I was stationed in
7 Thailand flying the reconnaissance missions over Laos and
8 Cambodia in 1970 and 1971.

9 Senator McCaskill: And would you say that your
10 experience in the military and especially your service for the
11 government has always been for either political party and
12 apolitical in terms of your mission and your job?

13 Director Clapper: Absolutely. I have served -- I toiled
14 in the trenches in intelligence for every President since
15 President Kennedy. I have served as a political appointee in
16 both Republican and Democratic administrations. I am
17 apolitical.

18 Senator McCaskill: And by the way, without getting into
19 classified information, there are thousands of men and women
20 who are working in the intelligence community right now,
21 General Clapper. Correct?

22 Director Clapper: Absolutely.

23 Senator McCaskill: And would you say that their
24 experience in many instances mirrors yours, in terms of
25 military experience, many of them being either active military

1 or retired military?

2 Director Clapper: Yes. A large part of the intelligence
3 community workforce are military, and of course, there are
4 many former military, either those who completed full careers
5 or those who served enlistments briefly and then came to the
6 intelligence community as civilians.

7 Senator McCaskill: Would you think it any less important
8 that we maintain the intelligence community as a foundational,
9 apolitical bloc of our country in terms of its protection?

10 Director Clapper: I could not feel stronger about
11 exactly that. I think it is hugely important that the
12 intelligence community conduct itself and be seen as
13 independent, providing unvarnished, untainted, objective,
14 accurate, and timely and relevant intelligence support to all
15 policymakers, commanders, diplomats, et cetera.

16 Senator McCaskill: Do, in fact, members of the
17 intelligence community engage in life-threatening and very
18 dangerous missions every day, particularly as it relates to
19 the war on terror?

20 Director Clapper: You only need to walk into the lobby
21 of CIA and look at the stars on the wall or the front lobby of
22 NSA, and the number of intelligence people that have paid the
23 ultimate price in the service of their country.

24 Senator McCaskill: So let us talk about who benefits
25 from a President-elect trashing the intelligence community.

1 Who benefits from that, Director Clapper? The American
2 people, them losing confidence in the intelligence community
3 and the work of the intelligence community? Who actually is
4 the benefactor of someone who is about to become commander-in-
5 chief trashing the intelligence community?

6 Director Clapper: I think there is an important
7 distinction here between healthy skepticism, which
8 policymakers, to include policymaker number 1, should always
9 have for intelligence, but I think there is a difference
10 between skepticism and disparagement.

11 Senator McCaskill: And I assume the biggest benefactors
12 of the American people having less confidence in the
13 intelligence community are in fact the actors you have named
14 today, Iran, North Korea, China, Russia, and ISIS.

15 Director Clapper: The intelligence community is not
16 perfect. We are an organization of human beings, and we are
17 prone sometimes to make errors. I do not think the
18 intelligence community gets the credit it is due for what it
19 does day in and day out to keep this Nation safe and secure in
20 the number of plots, just one example, terrorist plots that
21 have been thwarted, both those focused on this country and
22 other countries.

23 Senator McCaskill: I want to thank the chairman and I
24 want to thank Senator Graham and others. There have been
25 others I can count on maybe a little bit more than one hand

1 who have stood up in a nonpolitical way to defend the
2 intelligence community over the last few weeks. The notion
3 that the soon-elected leader of this country would put Julian
4 Assange on a pedestal compared to the men and women of the
5 intelligence community and the military that is so deeply
6 embedded in the intelligence community -- I think it should
7 bring about a hue and cry no matter whether you are a
8 Republican or a Democrat. There should be howls. And mark my
9 word. If the roles were reversed, there would be howls from
10 the Republican side of the aisle.

11 Thank you, Mr. Chairman.

12 Chairman McCain: Thank you for that nonpartisan comment.

13 [Laughter.]

14 Chairman McCain: Director Clapper, how would you
15 describe Mr. Assange?

16 Director Clapper: How would I describe?

17 Chairman McCain: Mr. Assange.

18 Director Clapper: Well, he is holed up in the Ecuadorian
19 embassy in London because he is under indictment I believe by
20 the Swedish Government for a sexual crime. He has, in the
21 interests of ostensibly openness and transparency exposed in
22 his prior exposures, put people at risk by his doing that. So
23 I do not think those of us in the intelligence community have
24 a whole lot of respect for him.

25 Chairman McCain: Admiral?

1 Admiral Rogers: I would echo those comments.

2 Chairman McCain: Thank you.

3 Senator Fischer?

4 Senator Fischer: Thank you, Mr. Chairman.

5 And thank you, gentlemen, for being here today and I do
6 thank you for your service.

7 Gentlemen, as you all know, about a year ago, Congress
8 passed the Cybersecurity Information Sharing Act. And,
9 Director Clapper, could you comment on what steps have been
10 taken to implement the act in particular to provide cyber
11 threat information in the possession of the Federal Government
12 to non-government entities?

13 Director Clapper: There has been a lot of work done --
14 and this is principally through both the FBI and Department of
15 Homeland Security -- to share more broadly with the private
16 sector. Prior to the enactment of this act, I think this has
17 been a theme that we have all worked hard. Certainly one of
18 the reasons for the creation of the Office of Director of
19 National Intelligence was to assume a domestic role as well
20 and to promote sharing as much as we can. I think a lot of
21 improvement has been made, as I look back over the last 15
22 years, but there is more work to do.

23 So we have done a lot of work with, for example, fusion
24 centers, the 76 or so fusion centers that exist throughout the
25 country, to convey more information to them. I have a network

1 of 12 domestic DNI reps, Director of National Intelligence
2 representatives, which are FBI special agents in charge. And
3 we work through them, those instrumentalities, on a regional
4 basis to convey more information particularly on cyber threats
5 to State and local officials, as well as the private sector.

6 Senator Fischer: Thank you, sir.

7 Admiral Rogers, what is your assessment of the current
8 state of information sharing between the government and the
9 private sector, especially regarding cybersecurity threats?
10 And more importantly, what is the appropriate level of
11 expectation to have with respect to that information sharing?

12 Admiral Rogers: So in some ways I would characterize it
13 as uneven. Some sector relationships, as you heard General
14 Clapper talk about, the 16 sectors within the critical
15 infrastructure of our Nation -- in some sectors, the
16 relationship is very mature. Information tends to flow very
17 regularly. Other sectors, it is not quite as mature. I think
18 the positive side is, with the legislation, we have now
19 developed a framework for how we do it. I still am concerned
20 on the government side. I will only speak for NSA and Cyber
21 Command. On the government side, I am not entirely
22 comfortable that the products that I am generating are
23 optimized to achieve outcomes for our private counterparts. I
24 am always trying to remind our team our success needs to be
25 defined by the customer, not what we think is the right format

1 or the right things to share.

2 Senator Fischer: Do you think there is any additional
3 legislation that is going to be required? I guess I am
4 asking, what do you need? Do you think there are proper
5 authorities that are currently in place, or do we need new
6 legislation? Or do you guys just need to improve on your
7 execution of it?

8 Admiral Rogers: Probably all of the above, to be very
9 honest.

10 I look at what are the changes that we are going to need
11 collectively to create the workforce of the future. I work
12 within the DOD in an intel framework. But I would argue this
13 is kind of universal. It does not matter where you are
14 working. Where does the structure -- what is the recruitment
15 and the benefit process that we need to retain and attract a
16 workforce?

17 I am curious with the new administration coming in their
18 broad view of roles and responsibilities -- are they
19 comfortable with the current structure? Will their view be
20 that we need to fundamentally relook at something different? I
21 would be the first to acknowledge, as I previously said this
22 morning, we have got to get faster. We have got to get
23 faster.

24 Senator Fischer: You know, you have talked about case by
25 case and the ad hoc nature of our policies when it comes to

1 cyberspace before this committee many, many times, and that
2 has been an issue that this committee and the ETC Subcommittee
3 in particular has tried to address by requiring strategies so
4 that we can deter these hostile actors and delegations of
5 authority, a definition of what an act of war in cyberspace
6 is. You know, we can go on and on. The chairman just
7 mentioned we do not have a strategy. Some of us just do not
8 feel there is a strategy that is laid out there.

9 When you talk about speed and dealing with cyber attacks,
10 I assume you are just referring to our agencies in responding
11 to attack that is directly upon us. Do you think there needs
12 to be any kind of consensus-building on the international
13 stage with our allies in order to increase speed, or would
14 that delay it even more trying to run this through channels in
15 trying to respond quickly? Do we reach out to allies, or do
16 we perform our first duty in protecting this country?

17 Admiral Rogers: So we routinely do that now. You
18 clearly have highlighted it is a bit of a double-edged sword.
19 But it goes to the point from my perspective, cyber just does
20 not recognize many of these boundaries. And so when you are
21 trying to deal with an incident, is this something that is
22 really truly totally domestic, or has it originated from
23 somewhere external to our Nation? What kind of infrastructure
24 did it pass through? There is a whole lot of complexity to
25 this. So I apologize. It is not a simple binary choice

1 there, even as I acknowledge there are tradeoffs.

2 Senator Fischer: Thank you.

3 Thank you, Mr. Chair.

4 Chairman McCain: Senator Blumenthal?

5 Senator Blumenthal: Thanks, Mr. Chairman.

6 I want to join Senator McCaskill in expressing my
7 appreciation for the service of our intelligence community and
8 to you, Mr. Chairman, for your very strong and courageous
9 statements in support of the work of this committee to give
10 credit and credibility to that intelligence community and to
11 your statements also about the importance of cyber warfare.
12 It is not the first time we have been here on this topic, and
13 you have been resolute and steadfast in seeking to elevate
14 public awareness and public consciousness about the importance
15 of cyber attacks on this country and the threat of cyber
16 warfare.

17 And I want to explore a little bit why these very
18 demeaning and dismissive comments about our intelligence
19 community are so dangerous to our Nation. Is it not true, Mr.
20 Clapper, that public support for robust responses to cyber
21 attacks on our Nation depends on the credibility of our
22 intelligence community and dismissing the conclusions, very
23 credible and significant conclusions, about the Russian attack
24 undermines public support for actions that the President must
25 take to deter and punish these kinds of actions?

1 Director Clapper: I do think that public trust and
2 confidence in the intelligence community is crucial, both in
3 this country and I think the dependence that other countries,
4 other nations, have on the U.S. intelligence community. And I
5 have received many expressions of concern from foreign
6 counterparts about the disparagement of the U.S. intelligence
7 community or, I should say, what has been interpreted as
8 disparagement of the intelligence community.

9 Senator Blumenthal: Well, there is no question about the
10 disparagement. There is no question about the dismissing and
11 demeaning of the intelligence community, entirely unmerited.
12 And would you agree, in light of your saying that you are even
13 more resolute now in your conclusion about Russian involvement
14 in this hacking, that comparing it to the judgment made about
15 weapons of mass destruction in the Iraq situation is totally a
16 red herring, totally wrong?

17 Director Clapper: Yes, I agree with that.

18 My fingerprints were on that national intelligence
19 estimate. I was in the community then. That was 13 years
20 ago. We have done many, many things to improve our processes,
21 particularly with respect to national intelligence estimates,
22 in order to prevent that from happening again.

23 Whatever else you want to say about the intelligence
24 community, it is a learning organization, and we do try to
25 learn lessons. It is a very difficult business and getting

1 harder all the time. And there will be mistakes. But what we
2 do try to do, as we did after the NIE from October 2002 on
3 weapons of mass destruction in Iraq, was to learn from that,
4 profit, and make change. And our posture, particularly with
5 respect to a very important document, the apex of our product
6 line, national intelligence estimates, it is the difference of
7 night and day.

8 Senator Blumenthal: I appreciate the extraordinary
9 humility of that statement, especially in light of the
10 excellence and expertise that your organization and you
11 personally have brought to this very, very difficult endeavor
12 to provide -- and I am quoting you I think -- unvarnished,
13 untainted, timely, accurate information to the most critical
14 national security decisions that this Nation makes. And I
15 want to express my appreciation for it and say that I think
16 some of the disparagement has been a terrible disservice to
17 our Nation and to the very brave and courageous men and women
18 who put their lives at risk so that this Nation can be better
19 informed in using our military and other force. So I hope
20 that we will see a change.

21 I also join the chairman in saying that we need better
22 policies on what constitutes a cyber attack on this Nation and
23 provide a more robust response, for example, against the
24 Russians not necessarily in cyber but to impose stronger
25 sanctions on their oil exports, on their use of foreign

1 exchange. The response to cyber attacks need not be one in
2 the cyber domain and in fact might be even more effective if
3 it hits their economy and their pocketbook and their
4 livelihoods.

5 So, Mr. Under Secretary, I appreciate your comments in
6 that regard. I do not know whether you want to comment in
7 response to what I have said. And I am out of time. So maybe
8 we can get that in writing.

9 [The information follows:]

10 [COMMITTEE INSERT]

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 Director Clapper: Senator Blumenthal, I do want to thank
2 you -- on behalf all the women and men of the intelligence
3 community, I want to thank you for that.

4 Senator Blumenthal: Thank you.

5 Chairman McCain: Senator Cotton?

6 Senator Cotton: Thank you all for appearing before us.

7 Mr. Secretary, Director Clapper, since this is your final
8 appearance, I know you hope, thank you very much for your many
9 years of service, Director Clapper, particularly you.

10 I will add my voice to Senators Blumenthal and McCaskill
11 in my admiration for the men and women in our intelligence
12 agencies. I have had a chance as a member of the Intelligence
13 Committee to meet them here at hearings and at their
14 headquarters around the world. And they do not get the credit
15 they often deserve. The troops that we help provide for in
16 this committee usually do because they wear uniforms and they
17 are known in public, but intelligence officers do not wear
18 uniforms and they are frequently undercover. So I want to
19 express my admiration and deepest respect and gratitude for
20 what they do.

21 We have heard a lot of imprecise language here today --
22 and it has been in the media as well -- phrases like "hacked
23 the election," "undermine democracy," "intervened in
24 election." So I want to be more precise here. Director
25 Clapper, let us go to the October 7th statement. That says,

1 quote, the recent compromises of emails from U.S. persons and
2 institutions, including from U.S. political organizations,
3 were instructed by the Russian Government. Are we talking
4 there specifically about the hack of the DNC and the hack of
5 John Podesta's emails?

6 Director Clapper: Yes.

7 Senator Cotton: Are we talking about anything else?

8 Director Clapper: That was essentially at the time what
9 we were talking about.

10 Senator Cotton: At the time then -- it says that the
11 recent disclosures through websites like DCLeaks and WikiLeaks
12 are consistent with the methods and motivations of Russian-
13 directed efforts. DNC emails were leaked first, I believe, in
14 July. Is that what the statement is talking about there?

15 Director Clapper: I believe so.

16 Senator Cotton: Mr. Podesta's emails I believe were not
17 leaked until that very day on October 7th. So was the
18 statement referring to that yet, or was that not intended to
19 be included?

20 Director Clapper: I would have to research the exact
21 chronology of when John Podesta's emails were compromised.
22 But I think, though, that bears on my statement that our
23 assessment now is that is even more resolute than it was with
24 that statement on the 7th of October.

25 Senator Cotton: Thank you.

1 Admiral Rogers, in November at the Wall Street Journal
2 Forum, you stated, quote, this was a conscious effort by a
3 nation state to attempt to achieve a specific effect. End
4 quote. By that, did you also refer to the hack of the DNC,
5 the hack of John Podesta's email and the leaks of those
6 emails?

7 Admiral Rogers: Yes.

8 Senator Cotton: Did you refer to anything else besides
9 those two things?

10 Admiral Rogers: To be honest, I do not remember the
11 specifics of that one particular 30-minute engagement, but
12 clearly what you outlined was part of my thought process.

13 Senator Cotton: Okay.

14 And then further on in that statement, Director Clapper,
15 the intelligence community says, quote, it would be extremely
16 difficult for someone, including a nation state actor, to
17 alter actual ballot counts or election results by cyber attack
18 or intrusion. End quote. And you stated that earlier today
19 as well, that we have no evidence that vote tallies were
20 altered or manipulated in any way.

21 Director Clapper: That is correct.

22 Senator Cotton: So that is what happened. Let us
23 discuss why.

24 Director Clapper, in response to Senator Nelson, you
25 stated that the report soon to be released will discuss the

1 motive. Would you care to give any kind of preview today?

2 Director Clapper: I would rather not.

3 Senator Cotton: I did not think so.

4 Director Clapper: There is actually more than one
5 motive. So that will be described in the report.

6 Senator Cotton: In your 53 years of intelligence, is
7 ascertaining the motives, plans, and intentions of foreign
8 leaders among the hardest tasks that we ask our intelligence
9 services to perform?

10 Director Clapper: It always has been.

11 Senator Cotton: There is a widespread assumption -- this
12 has been expressed by Secretary Clinton herself since the
13 election -- that Vladimir Putin favored Donald Trump in this
14 election. Donald Trump has proposed to increase our defense
15 budget to accelerate nuclear modernization and to accelerate
16 ballistic missile defenses and to expand and accelerate oil
17 and gas production which would obviously harm Russia's
18 economy. Hillary Clinton opposed or at least was not as
19 enthusiastic about all those measures.

20 Would each of those put the United States in a strong
21 strategic position against Russia?

22 Director Clapper: Well, certainly anything we do to
23 enhance our military capabilities, absolutely.

24 Senator Cotton: There is some contrary evidence, despite
25 what the media speculates, that perhaps Donald Trump is not

1 the best candidate for Russia.

2 Okay. So that is what happened. That is why it
3 happened, or at least a preview that we are going to know why
4 it happened. Let us move on to the impact.

5 Director Clapper, you said to Senator McCain earlier,
6 quote, the intelligence community cannot gauge the impact, end
7 quote, on the election. Is that because that kind of
8 electoral analysis is not a task that is within the
9 traditional responsibility and skill sets of intelligence
10 services?

11 Director Clapper: That is correct.

12 Senator Cotton: That is something that is more suited
13 for someone Shawn Hannity or Michael Barone or Nate Silver,
14 election analysts that have written extensively on the
15 election.

16 Director Clapper: Well, it certainly is not the purview
17 of the U.S. intelligence community.

18 Senator Cotton: Thank you.

19 Chairman McCain: Senator Heinrich?

20 Senator Heinrich: Thank you, Chairman.

21 Since this will likely be the last hearing that some of
22 you will attend in front of this committee, I just want to
23 thank you all for your service and thank all the men and women
24 who work for you. I want to say a special note of gratitude
25 to Director Clapper for 50 years of incredible service to this

1 country.

2 I think what makes America great has been our ability to
3 elect leaders through a fair, through a peaceful and a
4 transparent process without fear of rigging or interference in
5 elections. And unfortunately, in this past election, we know
6 that interference occurred. And when I say "interference," I
7 want to be specific. It is not about someone physically
8 stuffing ballot boxes or someone hacking our electronic voting
9 machines to give one candidate more votes than the other. It
10 is about selectively and deliberately releasing damaging
11 information in hopes of furthering one's strategic objectives,
12 in this case, Russia's strategic objectives.

13 I believe this is going to happen again unless there is a
14 price to be paid. This interference impacts the foundation of
15 our democracy, our elections, which is why I welcomed the
16 sanctions against Russia announced by the President and why I
17 believe we need to be evaluating additional Russian sanctions.
18 It is simply too important for both parties and for the future
19 of our country.

20 Secretary Lettre, given the need for deterrence in this
21 atmosphere which, as you said, is not always achieved by a
22 cyber response, how important are tools like sanctions to
23 imposing the kind of clear costs that you articulated?

24 Mr. Lettre: Sanctions are a very useful tool in that
25 toolkit. And I think in the case of the current situation

1 that we find ourselves in, it would be prudent to continue to
2 look at other options to impose more sanctions on Russian
3 actors as the facts continue to develop.

4 Senator Heinrich: I would agree with that estimate and I
5 hope that folks on both sides of the aisle will be looking at
6 those additional tools.

7 For any of you who want to answer this, I would like to
8 know how has the President-elect's at least inferred
9 dismissive attitude towards the intelligence community broadly
10 impacted morale in your agencies?

11 Director Clapper: Well, I have not done a climate
12 survey, but I hardly think it helps it.

13 Senator Heinrich: Does anyone want to add to that?

14 Admiral Rogers: I do not want to lose good, motivated
15 people who want to help serve this Nation because they feel
16 they are not generating value to help that Nation. And I am
17 the first to acknowledge there is room for a wide range of
18 opinions of the results we generate. We do not question that
19 for one minute, and every intelligence professional knows
20 that. I have had plenty of times in my career when I have
21 presented my intelligence analysis to commanders and
22 policymakers, and they have just looked at me and said, hey,
23 Mike, thanks but that is not the way I see it or you are going
24 to have to sell me on this. That does not bother any of us.
25 What we do I think is relevant, and we realize that what we do

1 is in no small part driven in part by the confidence of our
2 leaders in what we do. And without that confidence, I just do
3 not want a situation where our workforce decides to walk
4 because I think that really is not a good place for us to be.

5 Senator Heinrich: I think many of us could not agree
6 more. And if the underlying facts that the intelligence
7 community brings us are incorrect, we should call that out. I
8 just have not seen any evidence indicating that in this case.
9 Oftentimes we come to different strategic or policy points of
10 view based on that information, but that is an entirely
11 different thing.

12 Director Clapper, I want to go to a little bit more of
13 not just the classified information, but the relevance of
14 publicly available information of the whole picture of
15 Russia's activities within the context of this election. Can
16 you talk a little bit about the activities of the Russian
17 Government's English language propaganda outlets, RT, Sputnik,
18 as well as the fake news activity we saw, as well as the
19 social media and how those paint a complete picture that is
20 supplemental to what we saw with the hacking in this case?

21 Director Clapper: I appreciate your raising that because
22 while there has been a lot of focus on the hacking, this was
23 actually part of a multi-faceted campaign that the Russians
24 mounted. And, of course, RT, which is heavily supported,
25 funded by the Russian Government, was very, very active in

1 promoting a particular point of view, disparaging our system,
2 our alleged hypocrisy about human rights, et cetera, et
3 cetera. Whatever crack, fissure they could find in our
4 tapestry, if you will, they would exploit it. And so all of
5 these other modes, whether it was RT, use of social media,
6 fake news -- they exercised all of those capabilities in
7 addition to the hacking. And, of course, the totality of that
8 I think, regardless of what the impact was which we cannot
9 gauge, just the totality of that effort not only as DNI but as
10 a citizen I think is of grave concern.

11 Senator Heinrich: Thank you, Mr. Chair.

12 Chairman McCain: Senator Ernst?

13 Senator Ernst: Thank you, Mr. Chair.

14 Gentlemen, thank you very much. I also want to thank you
15 and the men and women that work diligently in the intelligence
16 community for the work that they do for the United States of
17 America.

18 Admiral Rogers, you have stated twice now -- you have
19 really stressed this point -- that you must be faster and more
20 agile in your responses. And so our discussion this morning
21 will go back to a discussion that we had in September of this
22 last year in front of this body because I believe it is
23 important that you understand the capabilities that exist out
24 there and are readily available to the United States Cyber
25 Command.

1 This past September, I asked you about a Government
2 Accountability Office report that stated the Department of
3 Defense does not have visibility of all National Guard units'
4 cyber capabilities because the Department has not maintained a
5 database that identifies the National Guard units' cyber-
6 related emergency response capabilities, as required by law.

7 And I was a bit alarmed when you stated that you have not
8 seen the report. It was a report that took about a year to
9 compile and was presented to both this committee and the House
10 Armed Services Committee. And 4 months later, I still have
11 not received an answer from you, my questions for the record.
12 And all of this morning, all of the GAO recommendations are
13 still open from this report.

14 So it has been 4 months and I would just like an update
15 on that, if you have been able to read the report and where is
16 the Department at in regards to tracking National Guard cyber
17 capabilities?

18 Admiral Rogers: Yes, ma'am. So, first, we did not get
19 your question until December, but I acknowledge that you have
20 formally asked us this.

21 First, as U.S. Cyber Command, I am the operational
22 commander. Manning, training, and equipping is a function of
23 services and the Department. For me in my role, I track the
24 operational readiness levels of all National Guard and Reserve
25 units that are allocated to the mission force. So I bore into

1 them in the exact same way I do the active side.

2 In terms of more broadly, how is the Department tracking
3 the set of skills that are available both in the Reserve
4 component, I would argue it is the same challenges that are in
5 the active component. How do you take advantage of the
6 breadth of capability that is broader than just a particular
7 military occupational specialty, for example? And I am the
8 first to acknowledge, after talking to my teammates at OSD and
9 the services, I do not think we have a good answer for you. I
10 will have something in writing for you within the next week or
11 so because I do acknowledge that we need to do that.

12 Senator Ernst: I do appreciate that because how long has
13 the United States been experiencing attacks from entities
14 outside of the United States.

15 Admiral Rogers: You could argue we have been in this
16 cyber dynamic for over a decade. It has gotten worse.

17 Senator Ernst: A decade. And so we have taken the steps
18 of developing Cyber Command and the capabilities that exist
19 both in our Reserves, National Guard, and the active component
20 units. And to become faster and more agile, we need to know
21 what those capabilities are. So if you have a solution to
22 that on how we can track those capabilities, we need to figure
23 that out. Many of these units have the capability of
24 defending networks and yet we are not utilizing those
25 capabilities. And we do not know where they exist, to be

1 honest.

2 Admiral Rogers: So please do not take from my comment
3 that we do not believe that the role of the Guard and Reserve
4 is not important. If you look in the last 12 months, we have
5 got two cyber protection teams from the Guard that have been
6 mobilized. We have brought online in the Guard and the
7 Reserve national mission teams for the first time within the
8 last year. I mean, it is great to see how the Guard and
9 Reserve are developing more and more capability. That is a
10 real strength for us.

11 Senator Ernst: Absolutely, and I think we will continue
12 to see those develop even more in the future, but we need to
13 be able to utilize those capabilities that exist out there.

14 So you know that many of our best soldiers in the
15 National Guard and Reserve come from the private sector. I
16 know this from some of my own guardsmen that work full-time in
17 computer technology and cyber technology. And you stated in
18 September, you were trying to figure out how better to
19 leverage the National Guard. And do you have a response for
20 that? Have you thought of ways that we might be able to use
21 those Guard units more readily?

22 Admiral Rogers: This is a topic that in fact I just was
23 talking to General Lengyel, the Director of the Guard Bureau,
24 a few weeks ago to say, hey, look, this is something in 2017 I
25 want us to sit down. I think there is a couple of specific

1 mission areas where the capabilities of the Guard and Reserve
2 are really well optimized because I would be the first to
3 admit the answer cannot be every time we will just throw the
4 active component at this. I do not think that is an optimal
5 approach for us to do in business.

6 So you will see this play out for us in 2017. We got to
7 work through the Title 32 versus Title 10 issue, what role,
8 what is the right way to do this.

9 Senator Ernst: Absolutely.

10 Admiral Rogers: Do we put it within the defense support
11 to civil authority construct? I would like that because it is
12 a framework that we already have. I am a big fan of let us
13 not reinvent the wheel when it comes to cyber, how do we take
14 advantage of processes and the structures and authorities that
15 are already in place. That is one thing you will see some
16 specific changes on within the Department. We are working
17 through that right now on the policy side.

18 Senator Ernst: Very good. Well, I appreciate it. I
19 know my time is expiring. So I look forward to working with
20 you on that, Admiral Rogers.

21 Chairman McCain: Senator Donnelly?

22 Senator Donnelly: Thank you, Mr. Chairman.

23 And I want to thank all of you for all your efforts
24 today, for the amazing careers you have had.

25 And, Mr. Chairman, thank you for holding this hearing. I

1 think it is critically important to our Nation. And I want to
2 be clear that the purpose of today's hearing is not to debate
3 the validity of the election, but to discuss foreign attempts
4 to use cyber attacks to attack our country, including the
5 recent Russian actions intended to influence our elections.
6 And I appreciate the bipartisan effort to get our people the
7 answers they deserve.

8 And I am grateful for the amazing efforts that our
9 intelligence agencies put forth every single day, that every
10 day lives are on the line to make sure that we are safe and to
11 make sure that all Americans have a chance to take care of
12 their families and go to sleep at night and not have to worry
13 while your people are on the front lines all around the world.
14 I can tell you on behalf all Hoosiers that when it comes down
15 to a choice between your people, our intelligence agencies,
16 and Julian Assange, we are on your team every time. And I
17 actually find it stunning that there is even a discussion in
18 our country about the credibility of our intelligence agencies
19 versus Mr. Assange. It is astounding to me that we would even
20 make that comparison when you see the stars in the CIA
21 headquarters of all the people who have lost their lives and
22 all who have lost their lives in our agencies to keep us safe.
23 Director Clapper, how would you describe your confidence
24 in attributing these attacks to the Russian Government as
25 opposed to someone in their basement?

1 Director Clapper: It is very high.

2 Senator Donnelly: The government has named those
3 responsible for the DNC hacks as APT-28 and APT-29, part of
4 the Russian intelligence services, the GRU and the FSB. Are
5 all these actors targeted by these two entities known to the
6 public, sir?

7 Director Clapper: I am sorry, sir. The question again?
8 Were all what?

9 Senator Donnelly: All the actors targeted by these two
10 entities, the GRU, the FSB, APT-28, 29 -- do we know
11 everybody? Have you told us who is involved, or are there
12 more that you cannot discuss at this time?

13 Director Clapper: Right. I do not think I can discuss
14 that in this forum.

15 Senator Donnelly: Okay.

16 How far up the chain, in what you can tell us, does this
17 go in regards to the Russians? At what level were the
18 instructions to take these actions given?

19 Director Clapper: Again, sir, I cannot speak to that in
20 this setting.

21 Senator Donnelly: Thank you.

22 Do you think we are communicating clearly to our
23 adversaries in a language that they will understand that the
24 costs will outweigh any gains they get if they try this again?
25 Not only you, Director, but the others, and how do we best

1 send that message, do you think?

2 Director Clapper: Well, certainly the sanctions that
3 have been imposed, the expulsion of the 35 intelligence
4 operatives, the closure of the two facilities which were used
5 for intelligence purposes, and the other sanctions that were
6 levied, I think does convey a message. It is open to debate
7 whether more should be done. I am a big fan of sanctions
8 against the Russians, but that is just me.

9 Senator Donnelly: Admiral, what would you say, sir?

10 Admiral Rogers: I would agree. I mean, the challenge
11 here is, look, I do not think it is in the best interest of
12 any of our nations to be in this confrontational approach to
13 doing business, and we have got to figure out how do we
14 articulate what is acceptable, what is no acceptable in a way
15 that enables us to move forward in a productive relationship.
16 That is not unique to the Russians. I would argue that that
17 is a challenge for us with a whole host of actors out there.
18 This has just, in some ways, been the poster child for this
19 challenge of late.

20 Director Clapper: I would add to that, if I may, that it
21 certainly would be a good thing if we could find areas where
22 our interests converge. I am speaking of ours and the
23 Russians. And we have done that in the past. So just to foot
24 stomp Admiral Rogers' point. But I think there is a threshold
25 of behavior that is just unacceptable, and somehow that has to

1 be conveyed.

2 Senator Donnelly: Well, I am out of time, but on behalf
3 of all the American people, we want to thank you. You have
4 dedicated your lives to keeping us safe, and we are incredibly
5 grateful for it.

6 Thank you, Mr. Chairman.

7 Chairman McCain: Senator Sullivan?

8 Senator Sullivan: Thank you, Mr. Chairman. And thank
9 you and the ranking member for holding this hearing.

10 And I also want to thank you, General Clapper, Mr.
11 Secretary, for your service, as this might be your last
12 hearing, and the men and women you lead.

13 You described in your testimony the increasing attacks we
14 are seeing not just from Russia but China and other actors,
15 Iran, North Korea, their increasing capabilities. The
16 chairman's opening statement pretty much stated that it is his
17 view -- and I certainly share the view -- that we are being
18 hit repeatedly because the benefits outweigh the costs for
19 those who are taking these actions against us. Do you agree
20 with that?

21 Director Clapper: I do and I think we all do. For
22 adversaries like -- I will just name -- North Korea and Iran,
23 it is relatively low-cost acts that can cause havoc. And what
24 I think we have seen over time is that they keep pushing the
25 envelope because as their capabilities improve and they are

1 willing to exercise those capabilities.

2 Senator Sullivan: So if that is the case -- I was glad
3 that I think there is some consensus here. You are talking
4 about retaliating, upping the costs with all instruments of
5 power, Mr. Secretary, you mentioned at the time of our
6 choosing, in the realm of our choosing. But it does not seem
7 to be happening. It does not seem to be happening because the
8 attacks continue.

9 So let me just give an example. Let us say Iran
10 conducted -- and you mentioned that they are being more
11 aggressive more risky than North Korea -- some kind of cyber
12 attack. If we did something maybe without announcing it, like
13 the President announced the Russian counteraction, but let us
14 say we did not announce it and let us say we did something
15 where we essentially collapsed their financial system or
16 something pretty dramatic. And we let them know
17 we did it, but we do not have to publicize it. Do you think
18 that is the kind of action that would say, hey, do not do this
19 or we are going to come back and retaliate at our time, our
20 choosing, and crush you? How come we have not done that yet,
21 and do you think if we did something like that with the
22 Iranians or the North Koreans, would that deter them in the
23 future, Mr. Secretary?

24 Mr. Lettre: Senator, I think you are getting right at
25 the question of what do we mean by a proportional response in

1 some instances.

2 Senator Sullivan: Or asymmetric. You are talking about
3 asymmetric responses, which I fully agree with.

4 Mr. Lettre: That is right. Or in instances that are
5 significantly serious and grave, whether a more than a
6 proportional response is required to really set that
7 deterrence framework in place.

8 Senator Sullivan: But is the key question not right now-
9 - it came from the chairman's opening statement, which I think
10 you agreed with -- is that nobody seems to be intimidated by
11 us right now.

12 So let me give another example. Senator Inhofe asked a
13 question early on about China. China hacked allegedly --
14 maybe you can confirm that -- government-led -- 22 million
15 files, a lot of the SF-86 files that you use for background
16 clearances. They have mine I was informed by the government.
17 Very sensitive information, as you know, that they could use
18 against intelligence operatives and military members. And
19 Senator Inhofe asked the question, what did we do? The answer
20 that I heard from all of you was, well, we try to protect
21 people like me and, I am sure, others whose sensitive intel
22 information and background information was compromised. But I
23 did not hear any claim of a retaliation on a huge hack --
24 huge. 22 million American Federal, military, intel workers
25 got hacked by the Chinese.

1 So the President signed this statement with President Xi
2 Jinping, the U.S.-China Security Agreement, but obviously,
3 General Clapper, from your testimony the Chinese have not
4 abided by that. Have they?

5 Director Clapper: They have.

6 Senator Sullivan: I am sorry. I thought you said in
7 your testimony today that they continue to conduct cyber
8 attacks.

9 Director Clapper: They continue to conduct cyber
10 espionage. They have curtailed -- as best we can tell, there
11 has been a reduction, and I think the private sector would
12 agree with this. There has been some reduction in their cyber
13 activity. And the agreement simply called for stopping such
14 exfiltration for commercial gain.

15 Senator Sullivan: So let me just ask a final question.
16 Did we retaliate and up the costs against China after an
17 enormous cyber attack against our Nation?

18 Director Clapper: We did not retaliate against an act of
19 espionage any more than other countries necessarily have
20 retaliated against us for when we conduct espionage.

21 Senator Sullivan: But is that answer not part of the
22 problem that we are showing that we are not going to make it
23 costly for them to come in and steal the files of 22 million
24 Americans, including many intel officers?

25 Director Clapper: Well, as I say, people who live in

1 glass houses need to think about throwing rocks because this
2 was an act of espionage. And we and other nations conduct
3 similar acts of espionage. So if we are going to punish each
4 other for acts of espionage, that is a different policy issue.

5 Chairman McCain: Senator King?

6 Senator King: Thank you, Mr. Chairman. Your opening
7 statements are always erudite and thoughtful, but I thought
8 today's was particularly so. You touched on all the important
9 points that have really formed the basis for this hearing. So
10 I want to thank you for that.

11 Director Clapper, I think it is important to put some
12 context around some of these discussions. One of the most
13 important things to me is that your public statement in
14 October, along with Jeh Johnson, was prior to the election,
15 and you were simply telling facts that you had observed. And
16 in my experience of reading intelligence community
17 communications, it is one of the more unequivocal that I have
18 seen. You have stated here you have high confidence in those
19 conclusions that the Russians were behind it, that it was
20 intended to interfere with our elections, and that approval
21 went to the highest levels of the Russian Government. Have
22 you learned anything subsequently that you can tell us here
23 today to contradict those findings that you publicly stated
24 last October?

25 Director Clapper: No. In fact, if anything, what we

1 have since learned just reinforces that statement of the 7th
2 of October.

3 Senator King: And there was no political intention. You
4 were simply reporting facts as you saw them. I presume that
5 is correct. Your history is one of being nonpolitical.

6 Director Clapper: Absolutely. I felt particularly
7 strongly, as did Secretary Johnson, that we owed it to the
8 American electorate to let them know what we knew.

9 Senator King: Now, people in Maine are skeptical and
10 they want to have evidence and proof. And I am hearing from
11 people, prove it. The problem, as I understand it, is the
12 desire to provide evidence that is convincing that your
13 conclusions are correct versus the danger of compromising
14 national security on sources and methods. Can you sort of
15 articulate that? Because I think that is an important point.

16 Director Clapper: We have invested billions, and we put
17 people's lives at risk to glean such information. And so if
18 we were to fulsomely expose it in such a way that would be
19 completely persuasive to everyone, then we can just kiss that
20 off because we will lose it, and then that will endanger our -
21 - imperil our ability to provide such intelligence in the
22 future. And that is the dilemma that we have in intelligence.
23 We want to be as forthcoming and transparent as possible, but
24 we feel very, very strongly, as we do in this case, about
25 protecting very fragile and sensitive sources and methods.

1 Senator King: Let us again turn to a question of
2 context. What we saw in this country this fall and going back
3 actually almost a year was an example of a Russian strategy
4 that has been playing out in Europe for some time that
5 includes not just hacking, as you said, but disinformation,
6 propaganda.

7 I heard just from a senior commander -- I took a break
8 here from the hearing -- in Europe that Russia is actually
9 buying commercial TV stations in western Europe at this point.
10 And this is a comprehensive strategy that we have seen playing
11 out in eastern Europe, and also there was a report this
12 morning that they are funding one of the candidates for the
13 presidency of France in the election this May.

14 Director Clapper: Well, the Russians have a long history
15 of interfering in elections, theirs and other people's. And
16 there is a long history in this country of disinformation.
17 This goes back to the 1960s, you know, the heyday of the Cold
18 War -- funding that they would share or provide to candidates
19 they supported, the use of disinformation. But I do not think
20 that we have ever encountered a more aggressive or direct
21 campaign to interfere in our election process than we have
22 seen in this case.

23 Senator King: And there are so many more channels of
24 disinformation today than there were in the past.

25 One final point.

1 Director Clapper: That is exactly right, and that is a
2 very key point about the -- of course, the cyber dimension and
3 social media and all these other modes of communication that
4 did not exist in the Cold War.

5 Senator King: One final point. We had a meeting with
6 the committee with a group of representatives from the Baltic
7 States, and I know the chairman was just in the Baltic States.
8 And they are just deluged with this. I mean, they have been
9 warning us about this for years, about the messing around with
10 elections. I said, so what do you do? How do you defend
11 yourself? And they said, well, we are trying to defend
12 ourselves in various ways, but the best defense is for our
13 public to know what is going on so they can take it with a
14 grain of salt. I thought that was a very interesting
15 observation because their people now say, oh, yeah, that is
16 just the Russians.

17 That is why I think public hearings like this and the
18 public discussion of this issue is so important because we are
19 not going to be able to prevent this altogether. But we need
20 to have our people understand when they are being manipulated.
21 Would you agree with that conclusion?

22 Director Clapper: Absolutely. That is why I felt so
23 strongly about the statement in October.

24 Senator King: Thank you.

25 Thank you, Mr. Chairman.

1 Chairman McCain: Just to follow up, General Clapper.
2 During the Cold War we had a strategy and we had Radio Free
3 Europe. We had Voice of America. Senator Graham, who will be
4 speaking next, will attest that in our recent trip they do not
5 have a strategy. They do not have a counter-propaganda -- the
6 United States of America I am talking about. And we have got
7 to develop that strategy even if it encompasses the Internet
8 and social media. But they are doing pretty significant stuff
9 particularly in the Baltics and Eastern Europe. Would you
10 agree, Senator Graham?

11 Senator Graham: Yes. I appreciate being before the
12 committee. Thank you.

13 [Laughter.]

14 Senator Graham: So, yes, I would.

15 Would you agree with me that Radio Free Europe is
16 outdated?

17 Director Clapper: I am frankly not up on --

18 Senator Graham: Well, it says "radio," and a lot of
19 people do not listen to the radio like they used to.

20 Director Clapper: Well, actually radio is a very popular
21 mode in many parts of the world.

22 Senator Graham: Radio is big in your world?

23 Director Clapper: In my world?

24 Senator Graham: Yes.

25 Director Clapper: Not so much.

1 Senator Graham: Yes. I do not listen to the radio much
2 either.

3 So the bottom line is you are going to be challenged
4 tomorrow by the President-elect. Are you okay with being
5 challenged?

6 Director Clapper: Absolutely.

7 Senator Graham: Do you both welcome it?

8 Director Clapper: We do.

9 Senator Graham: Do you think it is appropriate?

10 Director Clapper: We do.

11 Senator Graham: Are you ready for the task?

12 Director Clapper: I think so.

13 Senator Graham: Good.

14 Is there a difference between espionage and interfering
15 in an election?

16 Director Clapper: Yes. Espionage implies, to me at
17 least, a passive collection, and this was much more activist.

18 Senator Graham: So when it comes to espionage, we better
19 be careful about throwing rocks. When it comes to interfering
20 in our election, we better be ready to throw rocks. Do you
21 agree with that?

22 Director Clapper: That is a good metaphor.

23 Senator Graham: I think what Obama did was throw a
24 pebble. I am ready to throw a rock.

25 Would I be justified as a United States Senator taking

1 your information about Russia's involvement in our election
2 and what they are doing throughout the world and be more
3 aggressive than President Obama if I chose to?

4 Director Clapper: That is your choice, Senator.

5 Senator Graham: Do you think he was justified in
6 imposing new sanctions based on what Russia did?

7 Director Clapper: I do.

8 Senator Graham: So to those of you who want to throw
9 rocks, you are going to get a chance here soon, and if we do
10 not throw rocks, we are going to make a huge mistake.

11 Admiral Rogers, is this going to stop until we make the
12 cost higher?

13 Admiral Rogers: We have got to change the dynamic here
14 because we are on the wrong end of the cost equation.

15 Senator Graham: Yes. You got that right.

16 Could it be Republicans' next election?

17 Admiral Rogers: This is not about parties per se.

18 Senator Graham: Yes. It is not like we are so much
19 better at cybersecurity than Democrats.

20 Admiral Rogers: Right.

21 Senator Graham: Now, I do not know what Putin was up to,
22 but I do not remember anything about Trump in the election.

23 Now, if Trump goes after the Iranians, which I hope he
24 will, are they capable of doing this?

25 Admiral Rogers: They clearly have a range of cyber

1 capability and they have been willing to go offensively. We
2 have seen in the United States in the one dam.

3 Senator Graham: So if Trump takes on China, which I hope
4 he will, are they capable of doing this?

5 Admiral Rogers: Yes.

6 Senator Graham: So we got a chance as a Nation to lay
7 down a marker for all would-be adversaries. Do you agree with
8 that?

9 Admiral Rogers: Yes, and I would be the first to
10 acknowledge we need to think about this broadly.

11 Senator Graham: And we should take that opportunity
12 before it is too late.

13 Admiral Rogers: Yes, sir.

14 Senator Graham: Do you agree with me that the foundation
15 of democracy is political parties, and when one political
16 party is compromised, all of us are compromised?

17 Admiral Rogers: Yes, sir.

18 Senator Graham: All right.

19 Now, as to what to do, you say you think this was
20 approved at the highest level of government in Russia,
21 generally speaking. Is that right?

22 Director Clapper: That is what we said.

23 Senator Graham: Who is the highest level of government?

24 Director Clapper: Well, the highest is President Putin.

25 Senator Graham: Do you think a lot happens in Russia big

1 that he does not know about?

2 Director Clapper: Not very many.

3 Senator Graham: Yes. I do not think so.

4 Director Clapper: Certainly none that are politically
5 sensitive in another country.

6 Senator Graham: Okay.

7 Now, as we go forward and try to deter this behavior, we
8 are going to need your support now and in the future. So I
9 want to let the President-elect know that it is okay to
10 challenge the intel. You are absolutely right to want to do
11 so. But what I do not want you to do is undermine those who
12 are serving our Nation in this arena until you are absolutely
13 sure they need to be undermined. And I think they need to be
14 uplifted, not undermined.

15 North Korea. Let me give you an example of real world
16 stuff that he is going to have to deal with Trump. Do you
17 believe that North Korea is trying to develop an ICBM to hit
18 the United States or that could be used to hit the United
19 States?

20 Director Clapper: That could be, yes.

21 Senator Graham: Do you agree with that, Admiral Rogers?

22 Admiral Rogers: Yes.

23 Senator Graham: So when the North Korean leader says
24 that they are close to getting an ICBM, he is probably in the
25 realm of truth?

1 Admiral Rogers: He is certainly working aggressively to
2 do that.

3 Senator Graham: And if the President of the United
4 States says it will not happen, he is going to have to come to
5 you all to figure out how far along they are because you would
6 be his source for how far along they are. Is that right?

7 Director Clapper: I hope we would be the source.

8 Senator Graham: Yes. I hope he would talk to you too.
9 And here is what I hope he realizes, that if he has to take
10 action against North Korea, which he may have to do, I intend
11 to support him, but he needs to explain to the American people
12 why. And one of the explanations he will give is based on
13 what I was told by the people who are in the fight. And let
14 me tell you this. You do not wear uniforms, but you are in
15 the fight. And we are in a fight for our lives.

16 I just got back from the Baltics, Ukraine, and Georgia.
17 If you think it is bad here, you ought to go there.

18 So, ladies and gentlemen, it is time now not to throw
19 pebbles but to throw rocks. I wish we were not here. If it
20 were up to me, we would all live in peace, but Putin is up to
21 no good and he better be stopped. And, Mr. President-elect,
22 when you listen to these people, you can be skeptical but
23 understand they are the best among us and they are trying to
24 protect us.

25 Thank you all.

1 Chairman McCain: Would you have any response to that
2 diatribe?

3 [Laughter.]

4 Director Clapper: Senator Graham and I have had our
5 innings before, but I find myself in complete agreement with
6 what he just said and I appreciate it.

7 Chairman McCain: Thank you.

8 Director Clapper: Chairman McCain, if I might just pick
9 up on a comment of yours and that has to do with the
10 information fight, if you will. And this is strictly personal
11 opinion, not company policy. But I do think that we could do
12 with having a USIA on steroids, United States Information
13 Agency, to fight this information war a lot more aggressively
14 than I think we are doing right now.

15 Chairman McCain: You know, I agree, General, and I think
16 one of the areas where we are lacking and lagging more than
17 any other area is social media. We know these young people in
18 the Baltics are the same as young people here. They get their
19 information off the Internet, and we have really lagged behind
20 there.

21 Senator Gillibrand?

22 Senator Gillibrand: Thank you, Mr. Chairman and Mr.
23 Ranking Member, for hosting this very important hearing.

24 I want to follow on some of the questioning that Senator
25 Ernst started concerning the National Guard and cyber. I have

1 been pushing DOD to use the Guard for years and appreciate
2 that this is beginning to happen. Members of the Guard bring
3 unique skills and capabilities, and we should be leveraging
4 them.

5 Admiral Rogers, I look forward to working with you on how
6 best to do this. Can you tell me whether there has been
7 movement on the Army National Guard cyber protection teams
8 being included in the cyber mission forces?

9 Admiral Rogers: Yes. We brought two online that have
10 been activated in the last year, two additional that are
11 coming online in 2017, the first of which just came online.
12 So, yes, ma'am.

13 Senator Gillibrand: And how much more is left to be
14 done?

15 Admiral Rogers: The Guard and Reserve are bringing on an
16 additional 21 teams. Those will not be directly affiliated
17 with the mission force. But one of the things I think we are
18 going to find over time, the only way to generate more
19 capacity in a resource-constrained world is to view this as an
20 entire pie, not just, well, here is one sliced off area, the
21 mission force, and here is a separate area, the Guard and
22 Reserve. I think what we are going to be driven to is we are
23 going to have to look at this as much more integrated whole.

24 Senator Gillibrand: I do too because at the end of the
25 day, our Guard and Reserve -- they have day jobs and they may

1 be working at Google and Microsoft and Facebook and all these
2 technology companies and have extraordinary skills. And as a
3 way to tap into the best of the best, I think we should look
4 at people who already have these skills who are already
5 committed to serving our Nation as best we can. So I
6 appreciate your work.

7 Admiral Rogers: And if I could, one area that I would be
8 interested in your help in -- for many employers in the Guard
9 and Reserve -- and I say this as the son of guardsman when I
10 was a kid growing up -- they often -- sometimes -- tend to
11 view that service as something that you do overseas. Hey, I am
12 willing to let you go because you are going to Afghanistan,
13 you are going to Iraq. In the world of cyber, we are
14 operating globally from a garrison, pick the location--

15 Senator Gillibrand: From any location in the world.

16 Admiral Rogers: Anywhere.

17 This just came up. General Lengyel and I were just
18 talking about this yesterday, as a matter of fact. I said one
19 of the things we need to do is educate employers about what is
20 the nature of this dynamic, and it is every bit as relevant as
21 we are sending somebody to Afghanistan or Iraq.

22 Senator Gillibrand: I think that is right.

23 On a separate topic but related, I have long been
24 advocating for aggressive development of the manpower that we
25 need to support our cybersecurity mission. In particular, I

1 continue to believe that we have to not only develop the
2 capability in our military and the interest in cyber among
3 young Americans, but that the military must be creative when
4 thinking about recruitment and retention of cyber warriors.

5 How would you assess our current recruitment and
6 retention of cyber warriors? And what challenges do you
7 foresee in the future, and what recommendations do you have to
8 address them? Because, obviously, we are competing with some
9 of the most dynamic, innovative companies in the world, but we
10 need them to be our cyber defense and our cyber warriors.

11 Admiral Rogers: So knock on wood. In the military
12 aspect, we are exceeding both our recruiting and retention
13 expectations. I worry about how long can we sustain that over
14 time in the current model. My immediate concern is a little
15 less on the uniform side in part because if money was a
16 primary driver for them, they would not have come to us in the
17 first place.

18 On the civilian side, however, that is probably my more
19 immediate concern. I am finding it more challenging. We are
20 able to recruit well. Retaining them over time -- I am really
21 running into this on the NSA side right now. How do you
22 retain high-end, very exquisite civilian talent for extended
23 periods of time?

24 Senator Gillibrand: Well, I would be delighted to work
25 with you over the next year on that.

1 Director Clapper, I was very interested in your opening
2 remarks and the initial conversation you were having about the
3 Russian hack onto the DNC and to various personnels' emails
4 and the question of whether it was a declaration of war. And
5 given that that is such a serious statement, I want to ask
6 you, do you think we should take things like the Democratic or
7 Republican Party infrastructure and consider them to be
8 critical infrastructure? Should we actually be looking at our
9 infrastructure differently because of this recent event?

10 Director Clapper: That has been a subject of discussion
11 about whether, you know, our political infrastructure should
12 be considered critical infrastructure. I know Secretary
13 Johnson has had a discussion with State officials about that,
14 and there is some pushback on doing that. So it is a policy
15 call. Whatever additional protections that such a declaration
16 would afford, I think that would be a good thing. But whether
17 or not we should do that is really not a call for the
18 intelligence community to make.

19 Senator Gillibrand: Well, I hope it is one that the
20 members here on this committee will discuss because if it does
21 result in such a grave intrusion, maybe it should be critical
22 infrastructure. And certainly politics and political parties
23 are not set up that way, and so it would be quite a
24 significant change.

25 Thank you.

1 Chairman McCain: Director Clapper has to leave in about
2 20 minutes. So we will enforce the time.

3 Senator Tillis?

4 Senator Tillis: Thank you, Mr. Chair.

5 And, gentlemen, thank you all for your service. I for
6 one have high confidence in the community that you represent,
7 and I hope that they recognize that I speak for most of the
8 Senators here that share the same view.

9 Director Clapper, I am going to spend most my time
10 probably reflecting on some of the comments that you have
11 made. The glass house comment is something I think is very
12 important.

13 There has been research done by a professor up at
14 Carnegie-Mellon that has estimated that the United States has
15 been involved in one way or another in 81 different elections
16 since World War II. That does not include coups or regime
17 changes. So tangible evidence where we have tried to effect
18 an outcome to our purpose. Russia has done it some 36 times.
19 In fact, when Russia apparently was trying to influence our
20 election, we had the Israelis accusing us of trying to
21 influence their election. So I am not here to talk about
22 that, but I am here to say that we live in a big glass house
23 and there are a lot of rocks to throw. And I think that is
24 consistent with what you said on other matters.

25 I want to get back to the purpose of the meeting, the

1 foreign cyber threats. I think, Admiral Rogers and Director
2 Clapper, you all have this very difficult thing to communicate
3 to policy people who many not have subject-matter expertise in
4 this space. For example, Director Clapper, you were saying
5 that one of the problems with the counterattack -- I think it
6 was you. It could have been Admiral Rogers -- is that you may
7 have to use an asset that is actually a presence on some other
8 nation where that nation may or may not know that we have a
9 presence there. In fact, we have presences across cyberspace
10 that are not known that as a part of a counterattack, the
11 counterattack could be nothing more than exposing our
12 presences because we know a lot of our adversaries may or may
13 not be aware of presences that we have out there in
14 appropriate locations. Is that correct?

15 Director Clapper: Yes, and I think you have succinctly
16 illustrated the complexities that you run into here.

17 Senator Tillis: So that is why as thrilling as somebody
18 who has written the precursors to phishing code before and
19 stolen passwords as a part of ethical hack testings -- I was
20 paid to do this. That underscores the need for us to really
21 be educated about the nature of this battle space and how more
22 often than not, it is probably more prudent to seek a response
23 that is not a cyber response given the fluid nature.

24 We are in an environment now where we see a threat and we
25 build a weapon system. It is on the water. It is on the air.

1 It is on the ground. And then we kind of counter that threat
2 and we come up with war plans to use that capability.

3 In cyberspace, major weapon systems get created in 24-
4 hour cycles. You have no earthly idea whether or not you have
5 a defensive capability against them. So if you all of a
6 sudden think let us go declare war in cyberspace, be careful
7 what you ask for because collectively there are 30 nations
8 right now that have some level of cyber capability. There are
9 four or five of them that are near peer to the United States.
10 There are two or three that I think are very threatening and
11 in some cases probably have superior capabilities to us in
12 terms of presences, maybe not as sophisticated but potentially
13 in a cyber context more lethal.

14 So I think there are a lot of questions. One of the
15 beauties of being a freshman -- I guess now I am not a
16 freshman -- being at the end of the dais, all the good
17 questions have been asked. But one of the things that I would
18 suggest that we do is we as members really get educated on the
19 nature of this threat and the manner in which we go about
20 fighting it and understanding that the iterative nature of
21 weapons creations on the Internet are unlike anything we have
22 seen in record human history for warfare, and we need to
23 understand that.

24 We also need to understand what the rules of engagement
25 are going to be and how future AUMFs actually include a

1 specific treatment for behaviors that are considered acts of
2 war and then a whole litany of things that we should do for
3 appropriate responses so that we can begin to make more
4 tangible the consequences of inappropriate behavior in
5 cyberspace.

6 So that is not so much a diatribe, but it probably is a
7 speech, Mr. Chair.

8 The last thing I will leave you with is, Admiral Rogers,
9 I would like for my office to get with you and continue to
10 talk about how we get these bright people, retained and
11 recruited, to stay up to speed with developing these threats.
12 We need to understand that they are secret to creating these
13 weapon systems to counter the malicious acts like Russia,
14 China, Iran, and a number of other nations are trying to
15 develop against us.

16 Thank you.

17 Chairman McCain: Senator Hirono?

18 Senator Hirono: Thank you, Mr. Chairman.

19 And thank you, gentlemen, for your service.

20 I think it is clear that we have tremendous concerns
21 about the Russian hacking in our elections, and I think it is
22 more than ironic that we have a President-elect who kept
23 talking about our elections being rigged, which I would
24 consider trying to interfere with our elections to be a part
25 of a rigged kind of an election. At the same time, he denied

1 Russia's activities in this regard.

2 Some of this was already touched on regarding the
3 President-elect's attitudes toward the intelligence community,
4 the impact on morale. So going forward, as we are challenged
5 by the need to have more cyber-aware or skilled cyber
6 workforce, if this attitude toward the intelligence community
7 does not change on the part of decision-makers, including the
8 President, would you agree that it would make it that much
9 harder, Director Clapper and Admiral Rogers, to attract the
10 kind of cyber-experienced workforce that we need to protect
11 our country?

12 Director Clapper: Well, it could. I do not know that we
13 could say some of these statements have had any impact on
14 recruiting. It could.

15 Senator Hirono: Or retention.

16 Director Clapper: I think it could.

17 On retention, I think just maybe to embellish what
18 Admiral Rogers was saying, I do think that consideration needs
19 to be given to having more flexibility and more latitude on
20 compensation for our high-end cyber specialists who are lured
21 away by industry that are paying huge salaries. That is not
22 why you are in the government, not why you serve in the
23 intelligence community, not obviously for money. But I do
24 think in those highly technical, high-end skill sets that we
25 badly need in the government in the intelligence community,

1 that it would be helpful to have more latitude on
2 compensation.

3 Admiral Rogers: I would agree, Senator.

4 Senator Hirono: Very briefly.

5 Admiral Rogers: Both of these individuals know within
6 the last 24 hours, which I said using my authority as the
7 Director of NSA, I am going to authorize the following
8 increased compensations for the high-end cyber part of our
9 workforce because I am just watching the loss.

10 Senator Hirono: Yes, of course. And it is not just
11 compensation that attracts people to what we are doing in our
12 intelligence community because service to the country is a
13 very important motivation. And, of course, I would think that
14 morale would be very much attendant to that.

15 There was some discussion about what would constitute, in
16 the cyber arena, an act of war. Director Clapper, I note in
17 your testimony that I think this is one of the reasons that we
18 want to develop international norms in this arena. So who
19 should be the key players in developing agreeing to these
20 international norms in the cyber arena? And if the big
21 players are U.S., China, Russia, if we do not have those
22 players at the table to come up with these international
23 norms, how realistic is it to develop and --

24 Director Clapper: Well, that is exactly the challenge.
25 And those are the key nation states that we would need to

1 engage. And there has been work done under the auspices of
2 the United Nations to attempt to come up with cyber norms, but
3 I think we are a ways away from those having impact.

4 Senator Hirono: Would you agree, Admiral Rogers?

5 Admiral Rogers: Yes, ma'am.

6 Senator Hirono: Turning to the awareness of the public
7 as to the extent of the threat, a 2016 opinion piece by two
8 members of the 9/11 Commission -- basically they said that the
9 most important thing government and leaders in the private
10 sector can do is to clearly explain how severe this threat is
11 and what the stakes are for the country.

12 So, Director Clapper, do you think that the general
13 public understands the severity of the cyber threat and the
14 stakes for the country? And what should Americans keep in
15 mind with regard to this threat? And what can ordinary
16 Americans do to contend with this threat?

17 Director Clapper: I think there is always room for more
18 education, and certainly we have a role to play in the
19 intelligence community in sharing as much information as we
20 can on threats posed by both nation states, as well as non-
21 nation states.

22 And I think there are simple things that Americans can do
23 to protect themselves. You know, be aware of the threat posed
24 by spear phishing, for example, which is a very common tactic
25 that is used yet today. We have a challenge in the government

1 getting our people to respond appropriately to cyber threats.
2 So this is one case where communicate, communicate,
3 communicate is the watchword.

4 Chairman McCain: Senator Cruz?

5 Senator Cruz: Thank you, Mr. Chairman.

6 Gentlemen, thank you for being here. Thank you for your
7 service to our Nation.

8 The topic of this hearing, cybersecurity, cyber attack,
9 is a growing threat to this country and one that I think will
10 only become greater in the years ahead. We have seen in
11 recent years serious attacks from, among others, Russia,
12 China, North Korea. Indeed, it is with some irony -- I spent
13 a number of years in the private sector, and to the best of my
14 knowledge never had my information hacked. And then all I had
15 to do was get elected to the United States Senate and the
16 Office of Personnel Management was promptly hacked and
17 everyone on this bench had our information stolen by a foreign
18 assault.

19 My question, Admiral Rogers, starting with you is what do
20 you see as the greatest cybersecurity threats facing our
21 country, and what specifically should we be doing about it to
22 protect ourselves?

23 Admiral Rogers: So a small question.

24 When I look at the challenges and the threats, it is, in
25 no particular order, significant extraction of information and

1 insight that is generating economic advantage for others, that
2 is eroding operational advantage at times for us as a Nation.
3 That is, as you have seen in this Russian piece, where not
4 just the extraction but then the use of this information adds
5 a whole other dimension. And what concerns me beyond all that
6 is what happens as we start to move in an environment in which
7 not only is information being -- I have heard some people use
8 the phrase "weaponized." What happens when now we see people
9 suddenly manipulating our networks so we cannot believe the
10 data that we are looking at. That would be a real fundamental
11 game-changer to me, and to me it is only a question of the
12 "when" not the "if" this is going to happen. And what happens
13 when the non-state actor decides that cyber offers an
14 asymmetric advantage to them? Because their sense of risk and
15 their willingness to destroy the status quo is significantly
16 different and greater than your typical nation state. Those
17 are the kinds of long-term things.

18 So as we talked about more broadly today, we have got to
19 get better on the defensive side because part of deterrence is
20 making it harder for them to succeed. I acknowledge that.
21 But a defensive strategy alone is not going to work. It is a
22 resource-intensive approach to doing business, and it puts us
23 on the wrong end of the cost equation. That is a losing
24 strategy for us, but it is a component of a strategy. We have
25 got to ask ourselves how do we change this broader dynamic.

1 To go the point you have heard repeatedly today, how do we
2 convince nations and other actors out there that there is a
3 price to pay for this behavior, that in fact it is not in your
4 best interest.

5 Senator Cruz: And what should that price be?

6 Admiral Rogers: It is a wide range of things. There is
7 no one silver bullet, which is another point I would make. If
8 we are looking for the perfect solution, there is not one.
9 This will be a variety of incremental solutions and efforts
10 that are going to play out over time. There is no one single
11 approach here.

12 Senator Cruz: Well, and your point about manipulating
13 data, about a month ago I chaired in a different committee a
14 hearing on artificial intelligence and our economy's growing
15 reliance on artificial intelligence. And one of the things
16 that the witnesses testified there was concern on the
17 cybersecurity side of a hack that would modify the big data
18 that is being relied on for artificial intelligence to change
19 the decision-making in a way nobody is even aware it has been
20 changed. And I think that is a threat I hope that you all are
21 examining closely, and it is the sort of threat that could
22 have significant repercussions without anyone even being aware
23 it is happening.

24 Let me shift to a different topic. Director Clapper, you
25 have testified before this committee that Cuba is an

1 intelligence threat on par with Iran and listed below only
2 Russia and China. And there are reports that Lourdes, the
3 Russian-operated signal intelligence base in Cuba, will be
4 reopened. And additionally, this past summer Russia and
5 Nicaragua struck a deal to increase military and intelligence
6 cooperation, resulting in an influx of Russian tanks into
7 Managua and an agreement to build an electronic intelligence
8 base, which may be disguised as a satellite navigation
9 tracking station.

10 To the best of your knowledge, what is Russia's strategy
11 in the western hemisphere, and how concerned are you about the
12 Russians expanding their influence in Cuba and Nicaragua?

13 Director Clapper: Well, the Russians are bent on
14 establishing both a presence in the western hemisphere and
15 they are looking for opportunities to expand military
16 cooperation, sell equipment, airbases, as well as intelligence
17 gathering facilities. And so it is just another extension of
18 their aggressiveness in pursuing these interests.

19 And with respect to Cuba, Cuba has always had long-
20 standing, very capable intelligence capabilities, and I do not
21 see a reduction of those capabilities.

22 Senator Cruz: Thank you.

23 Chairman McCain: Senator Kaine?

24 Senator Kaine: Thank you, Mr. Chair.

25 And thanks to the witnesses for today and for your

1 service.

2 And, Mr. Chair, I appreciate you calling this hearing. I
3 think this hearing is a test of this body, the Article 1
4 branch of Congress, this hearing and others to follow.

5 I was chairman of the Democratic National Committee for a
6 couple years, and we had a file cabinet in the basement that
7 had a plaque over it. It was a file cabinet that was rifled
8 by burglars in an invasion of the Democratic National
9 Committee in 1972. It was a bungled effort to take some files
10 and plant some listening devices.

11 That small event led to one of the most searching and
12 momentous congressional inquiries in the history of this
13 country. It was not partisan. One of the leaders of the
14 congressional investigation was a great Virginian called Will
15 Butler, who was my father-in-law's law partner in Roanoke,
16 Virginia before he went to Congress, played a major role. It
17 was not an investigation driven because something affected the
18 election. The 1972 presidential election was the most one-
19 sided in the modern era. But it was a high moment for
20 Congress because Congress in a bipartisan way stood for the
21 principle that you could not undertake efforts to influence an
22 American presidential election and have there be no
23 consequence.

24 The item that we will discuss and we will discuss more
25 when the hearing comes out is different. That was a burglary

1 of a party headquarters that was directed to some degree from
2 the Office of the President. But this is very serious. The
3 combined intelligence of this country has concluded that
4 efforts were undertaken to influence an election by an
5 adversary, an adversary that General Joe Dunford, the head of
6 the Joint Chiefs of Staff, said in testimony before this
7 hearing, was in his view the principal adversary of the United
8 States at this point.

9 In addition, the attack was not just on a party
10 headquarters. The October 7 letter that you have referred to
11 talked about attacks on individuals, current and former public
12 officials with significant positions, and also attacks on
13 State boards of elections. The letter of October 7 traced
14 those attacks to Russian entities, Russian companies, and did
15 not ascribe, at least in that letter, to that directed by the
16 Russian Government, but I am curious about what the full
17 report will show.

18 It is my hope that this Congress is willing to stand in a
19 bipartisan way for the integrity of the American electoral
20 process and will show the same backbone and determination to
21 get all the facts and get them on the table, as the Congress
22 did in 1974.

23 There was another congressional inquiry that was directed
24 after the attacks on 9/11, and there was a powerful phrase in
25 that report that I just want to read. The commission

1 concluded, quote, the most important failure was one of
2 imagination. We do not believe leaders understood the gravity
3 of the threat. And that is something I think we will have to
4 grapple with. Did we have sufficient warning signs? I think
5 we did. And having had sufficient warning signs, why did we
6 not take it more seriously? That question is every bit as
7 important as a question about what a foreign government, an
8 adversary, did and how we can stop it from happening.

9 Three quick points.

10 One, is the report next week that is going to be issued
11 not solely going to be confined to issues of hacking but also
12 get into the dimension of this dissemination of fake news?
13 Will that be one of the subject matters covered?

14 Director Clapper: Without preempting the report, we will
15 describe the full range of activities that the Russians
16 undertook.

17 Senator Kaine: I think that is incredibly important.

18 I had a little role in this election. I was along for the
19 ride for 105 days and was the subject of a couple of fake news
20 stories. And it was interesting. There were at least three
21 that the mainstream media did not cover because they were so
22 incredible that like why would they. But I looked at one of
23 the stories that had been shared 800,000 times. And when I
24 see an administration who has put in place as the proposed
25 national security advisor someone who traffics in these fake

1 news stories and retweets them and shares them, who betrays a
2 sense of either gullibility or malice that would kind of be --
3 these are stories that most fourth graders would find
4 incredible. That a national security advisor would find them
5 believable enough to share them causes me great concern.

6 Second, go back to Joe Dunford. He talked about Russia
7 as a potential adversary because they have capacity and they
8 have intent. With respect to our cyber, I think we have
9 capacity, but I think what we have shown is we have not yet
10 developed an intent about how, when, why, whether we are going
11 to use the capacity we have. So if we are going to shore up
12 our cyber defense, in one word do you think what we really
13 need to shore up is our capacity, or do we need to shore up
14 our intent?

15 Director Clapper: As we look at foreign adversaries,
16 that is always the issue is capability and intent. And
17 certainly in the case of the Russians, they do pose an
18 existential threat to the United States. And I agree with
19 Chairman Dunford on that. It is probably not our place, at
20 least my place, in the intelligence community to do an
21 assessment of our intent. That is someone else's place. It
22 is not mine.

23 Chairman McCain: Senator Shaheen?

24 Senator Shaheen: Thank you, Mr. Chairman and Senator
25 Reed, for holding this hearing.

1 And thank you all very much for testifying this morning
2 and for your service to the country.

3 Dr. Robert Kagan testified before this committee last
4 December with respect to Russia. And at that time, there was
5 less information known to the public about what had happened
6 in their interference in the elections.

7 But one of the things he pointed out was that Russia is
8 looking at interference in elections, whether that be cyber or
9 otherwise, the whole messaging piece that you discussed with
10 Senator Heinrich, as another strategy along with their
11 military action and economic and other diplomatic methods to
12 undermine Western values, our Euro-Atlantic alliance, and he
13 very democracies that make up that alliance. Is that
14 something that you agree with, Director Clapper?

15 Director Clapper: Yes. That is clearly a theme. It is
16 certainly something that the Russians are pushing in messaging
17 in Europe. They would very much like to drive wedges between
18 us and Western Europe, the alliances there, and between and
19 among the countries in Europe.

20 Senator Shaheen: And I assume that there is agreement on
21 the panel. Does anybody disagree with that?

22 So one of the things that I think has emerged, as I have
23 listened to this discussion, is that we do not have a strategy
24 to respond to that kind of an effort. We do not have a
25 strategy, it has been testified, with respect to cyber, but a

1 broader strategy around messaging around how to respond to
2 that kind of activity. Do you agree with that?

3 Director Clapper: I am speaking personally.

4 Senator Shaheen: Sure.

5 Director Clapper: This is not an institutional response.
6 As I commented earlier to Senator McCain, I do think we need a
7 U.S. Information Agency on steroids that deals with the
8 totality of the information realm and to mount in all forums
9 and to include the social media.

10 Senator Shaheen: I am sorry to interrupt, but can I just
11 ask why do you believe that has not happened. Director
12 Clapper, Admiral Rogers?

13 Director Clapper: For my part, I do not know why it has
14 not. I cannot answer that.

15 Senator Shaheen: Admiral Rogers?

16 Admiral Rogers: From my perspective, in part because I
17 do not think we have come yet to a full recognition of the
18 idea that we are going to have to try to do something
19 fundamentally different. I think we still continue to try to
20 do some of the same traditional things we have done and
21 expecting to do the same thing over and over again, yet
22 achieve a different result.

23 Senator Shaheen: No. That is the definition of "crazy."
24 I think we have determined that.

25 Secretary Lettre?

1 Mr. Lettre: I would just add that in this area, the
2 capability and intent framework is useful to think about. I
3 think it is only in the last few years that we have seen
4 adversaries with true intent to use propaganda and the ability
5 to reach out as terrorists are doing and try to incite and
6 match that up with the tremendous power that social media
7 tools allow to make that easy and simple and effective and
8 broadly applicable.

9 Senator Shaheen: So given that this is a strategy and
10 given that it is aimed not just at the United States
11 particularly with respect to interference in our elections but
12 at Western Europe and Eastern Europe for that matter, is there
13 an effort underway to work with our allies through NATO or
14 otherwise? I have been to the cybersecurity center in
15 Estonia, but there did not seem to be a NATO agreement that
16 this was something that we should be working on together to
17 respond to. So is this an effort that is underway?

18 Mr. Lettre: Just speaking from my lens on things, there
19 is a lot of interest in doing that and doing it more
20 effectively and more comprehensively, but we have not cracked
21 the code on doing it effectively yet. And so we need to keep
22 the pressure on ourselves and our NATO allies who are
23 likeminded in this regard to keep improving our approach.

24 Admiral Rogers: And it has also got to be much broader
25 than just cyber.

1 Senator Shaheen: Thank you.

2 Director Clapper, my time is almost up, but before you go
3 since this is the last opportunity we will have to hear from
4 you, can I just ask you, do you think the DNI needs reform?

5 Director Clapper: Well, there is always room for
6 improvement. I would never say that this is the ultimate. I
7 do think it would be useful, though, if we are going to reform
8 or change the DNI or change CIA, that some attention be given
9 to, in our case, the legislative underpinnings that
10 established the DNI in the first place and then have added
11 additional functions and responsibilities over the years, that
12 the Congress has added, to our kit bag of duties. But to say
13 that there is not room for improvement, I would never suggest
14 that.

15 Senator Shaheen: I appreciate that. And I certainly
16 agree with you. I think that if there is going to be this
17 kind of major reform, hopefully both legislators and others
18 who have been engaged in the intelligence community will be
19 part of that effort.

20 Director Clapper: I certainly agree the Congress, no pun
21 intended, gets a vote here I think.

22 Senator Shaheen: Thank you.

23 Chairman McCain: I know that our time has expired, and I
24 apologize to our new members that you will not have time
25 because you have to go. But maybe, Director Clapper, since

1 this may be, hopefully, your last appearance, do you have any
2 reflections that you would like to provide us with,
3 particularly the role of Congress or the lack of the role of
4 Congress in your years of experience?

5 Director Clapper: I am going to have to be careful here.

6 Chairman McCain: I do not think you have to be.

7 [Laughter.]

8 Director Clapper: I was around in the intelligence
9 community when the oversight committees were first established
10 and have watched them and experienced them ever since.
11 Congress does have clearly an extremely important role to play
12 when it comes to oversight of intelligence activities, and
13 unlike many other endeavors of the government, much of what we
14 do, virtually all of what we do is done in secrecy. So the
15 Congress has a very important, a crucial responsibility on
16 behalf of the American people for overseeing what we do
17 particularly in terms of legality and protection of facilities
18 and privacy.

19 At risk of delving into a sensitive area, though, I do
20 think there is a difference between oversight and
21 micromanagement.

22 Chairman McCain: Well, we thank you. We thank the
23 witnesses. And this has been very helpful. Director Clapper,
24 we will be calling you again.

25 Director Clapper: Really?

1 [Laughter.]

2 Chairman McCain: This meeting is adjourned.

3 [Whereupon, at 12:09 p.m., the hearing was adjourned.]

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25