Kryptering

Utmaningar

bitsec

nixu cybersecurity.

<kahn >pedersen

C-Resiliens

TUTUS

Nationellt Sensorsystem

Mollitiam

Týr CYBER Defense

FÖRSVARSMAKTEN

SAAB

Office of Naval Research ONR Science & Technology

Säkerhetspolisen

REGERINGSKANSLIET

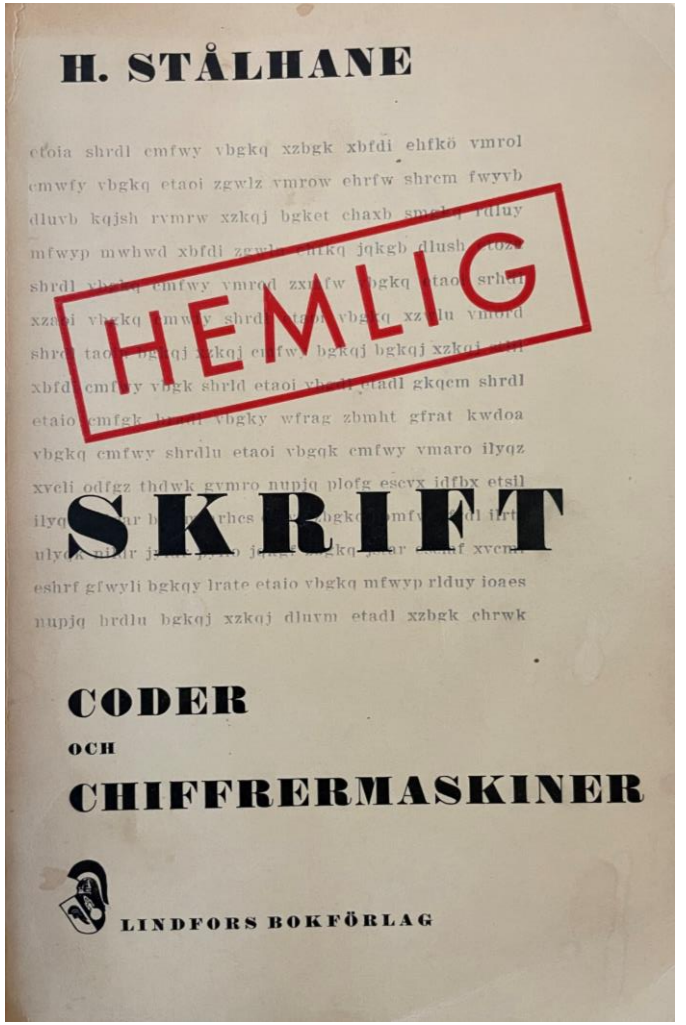
Посольство Швеции в Москве

André Catry

- **Entrepreneur**
  - C-Resiliens, Tutus Data, Mollitiam , Nationellt SensorSystem , Týr Cyber Defense
- **Author**
  - Honungsapan, Tigerögat, Solroskoden
- **Advisor**
  - Chief engineer / IT & Security Architect SAAB (Consultant)
  - Lawfirm Kahn Pedersen (Consultant)
- **Security expert /Lead Security Consultant**
  - IT & Security Architect / Investigator / Analyst / IT-Forensics
- **Security Consultant**
  - IT defense unit (ITF)
  - Military Intelligence & Security Service MUST (CERT)
- **Avdelningsdirektör (Principal administrative officer)**
  - IT security advisor to government agencies
  - Computer Forensics / Investigations
  - Lawful interception
- **Departementssekreterare (First Secretary, Desk Officer)**
  - IT security, 4 years embassy Moskva
  - Project manager

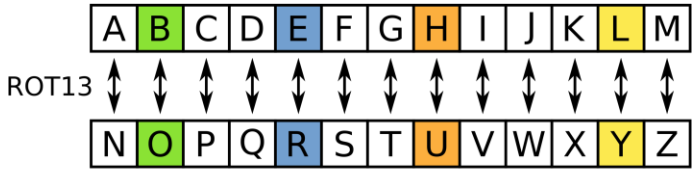
Kryptering är en svår materia

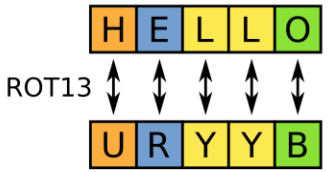
- Sveriges första bok som avhandlar kryptering utgiven 1934.

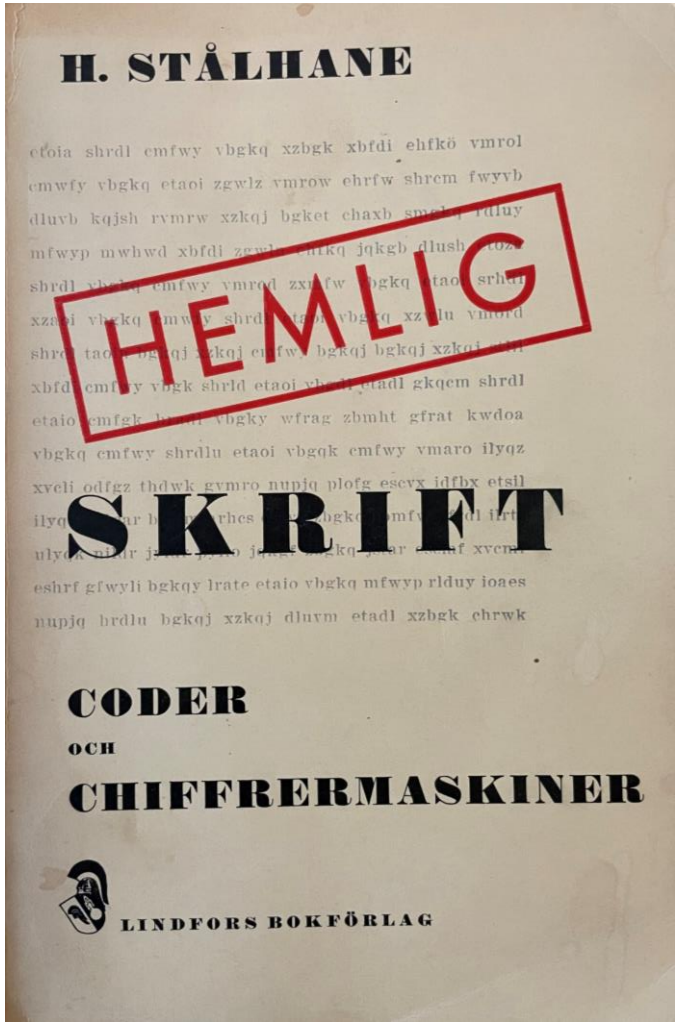


Kryptering är en svår materia

- Sveriges första bok som avhandlar kryptering utgiven 1934.

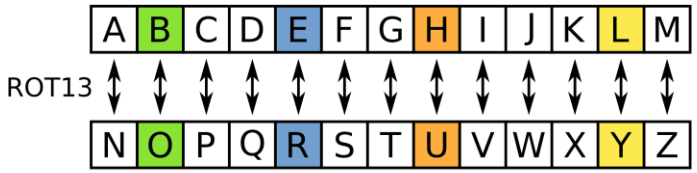


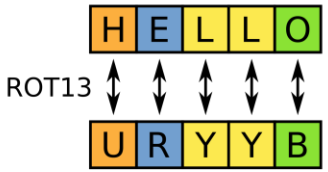




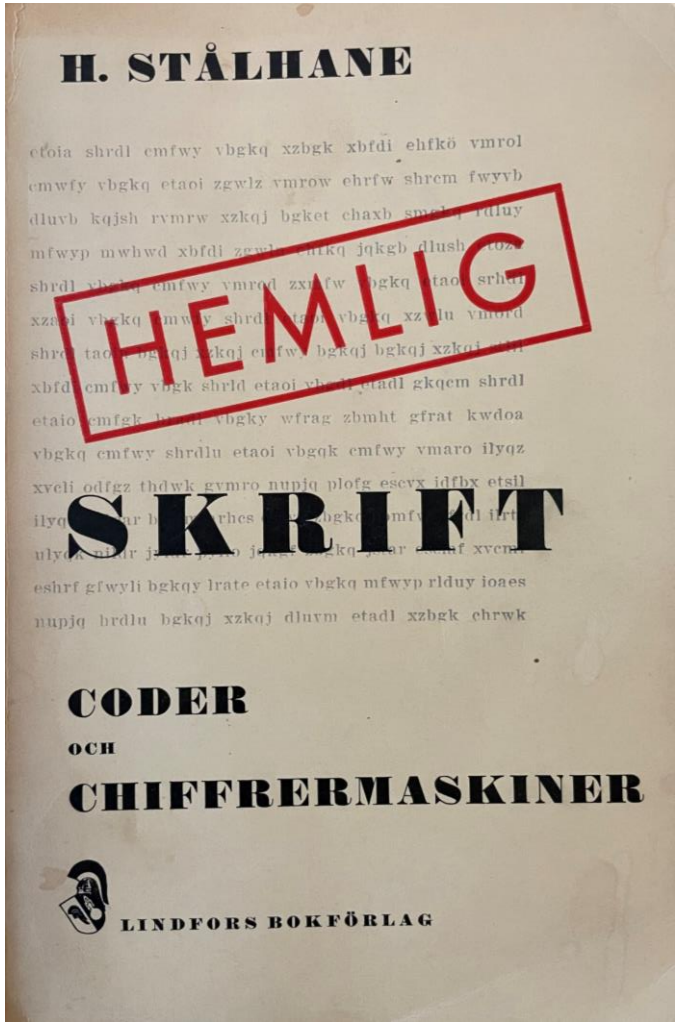
Kryptering är en svår materia

- Sveriges första bok som avhandlar kryptering utgiven 1934.





- Det som kanske var tillräckligt säker 1934 kan vi idag inte betrakta som kryptering.



AN

what is strong encryption

Strong encryption is the process of encoding data or information in such a way that it can only be accessed or read by someone who has the appropriate decryption key. The strength of encryption is determined by the algorithm used and the length of the encryption key. The longer the key and more complex the algorithm, the harder it is to decrypt the information without the key.

A good example of strong encryption is AES 256-bit encryption, which is widely used to protect sensitive data such as credit card information and personal information. This encryption method uses a 256-bit key and is considered to be practically unbreakable with current technology.

It's important to note that even though the encryption algorithm itself may be considered "strong", the security of the entire encryption system can be weakened if the key is not kept secret and if the implementation of the encryption is not secure.

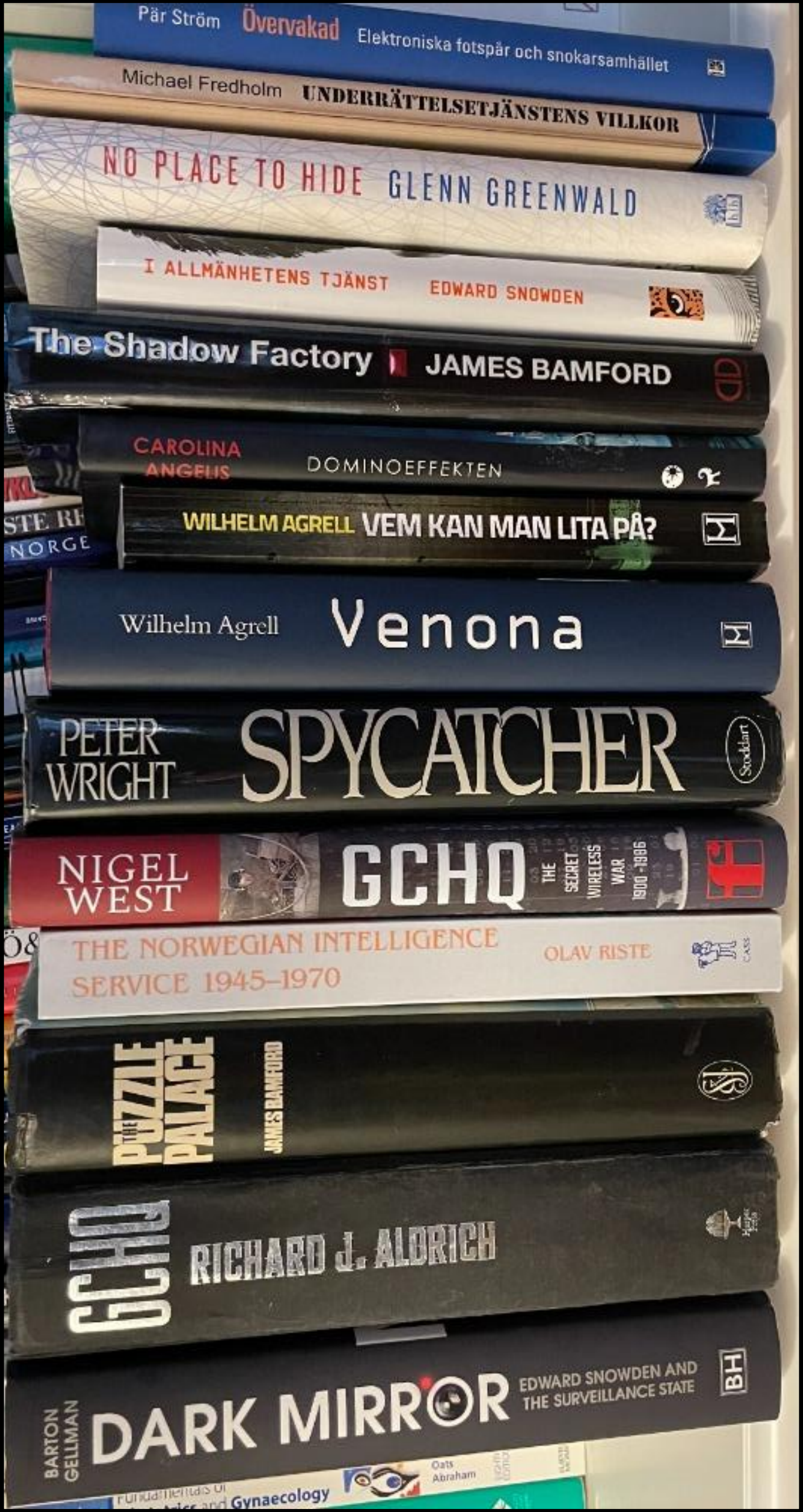
AN

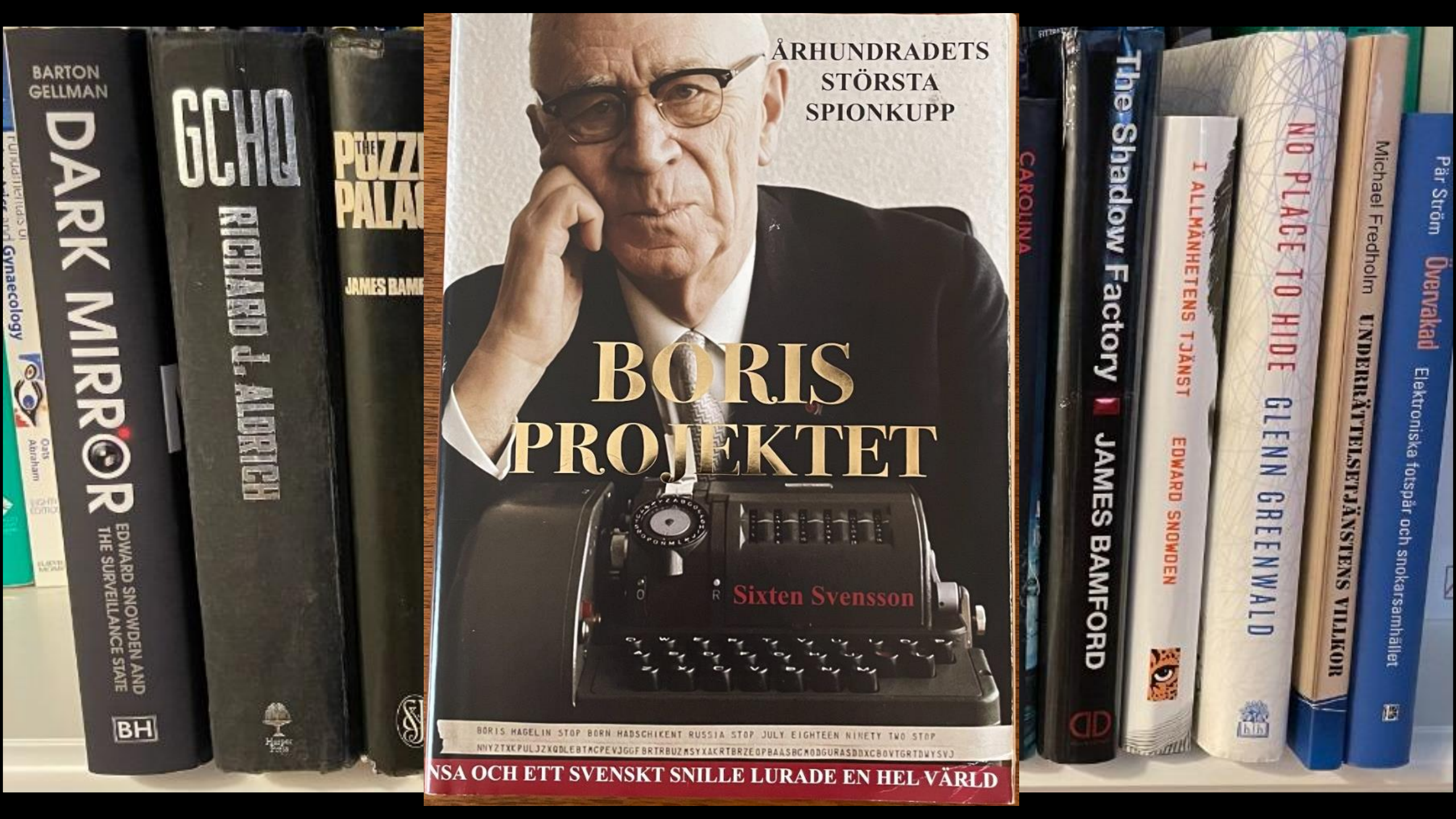
what is strong encryption

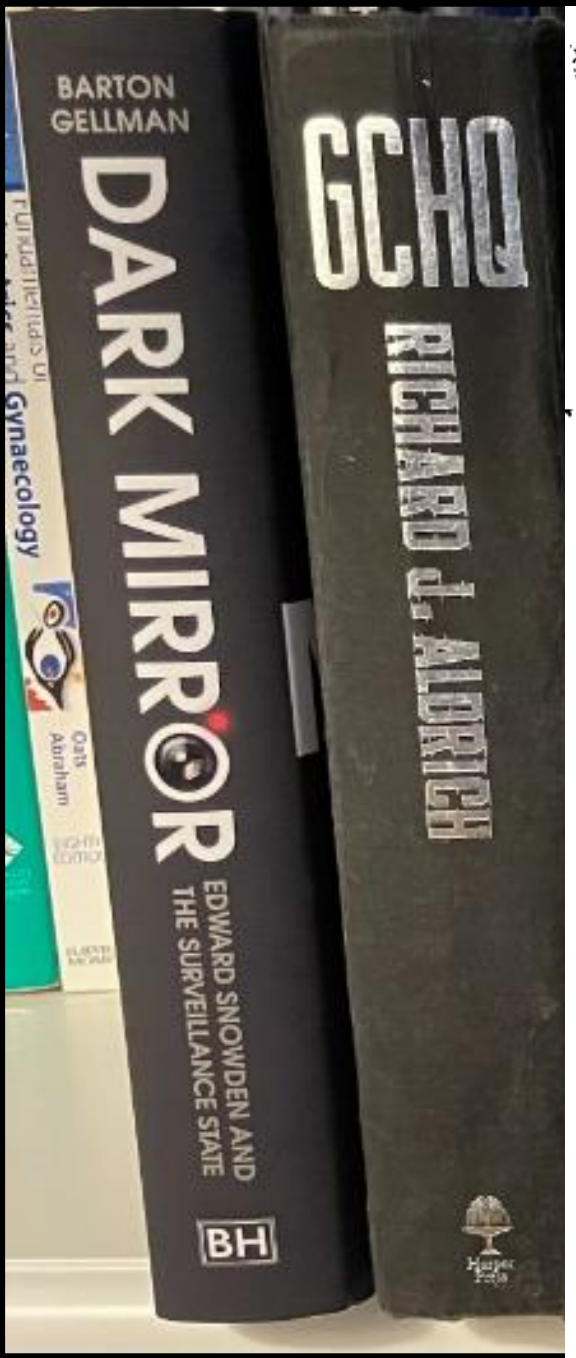
Strong encryption is the process of encoding data or information in such a way that it can only be accessed or read by someone who has the appropriate decryption key. The strength of encryption is determined by the algorithm used and the length of the encryption key. The longer the key and more complex the algorithm, the harder it is to decrypt the information without the key.

A good example of strong encryption is AES 256-bit encryption, which is widely used to protect sensitive data such as credit card information and personal information. This encryption method uses a 256-bit key and is considered to be practically unbreakable with current technology.

It's important to note that even though the encryption algorithm itself may be considered "strong", the security of the entire encryption system can be weakened if the key is not kept secret and if the implementation of the encryption is not secure.


Pär Ström
Övervakad
Elektroniska fotspår och snokarsamhället
Michael Fredholm
UNDERRÄTTELSETJÄNSTENS VILLKOR
NO PLACE TO HIDE
GLENN GREENWALD
I ALLMÄNHETENS TJÄNST
EDWARD SNOWDEN
The Shadow Factory
JAMES BAMFORD
CAROLINA ANGELIS
DOMINOEFFEKTEN
WILHELM AGRELL
VEM KAN MAN LITA PÅ?
Wilhelm Agrell
Venona
PETER WRIGHT
SPYCATCHER
NIGEL WEST
GCHQ
THE SECRET WIRELESS WAR 1900-1986
THE NORWEGIAN INTELLIGENCE SERVICE 1945–1970
OLAV RISTE
THE PUZZLE PALACE
JAMES BAMFORD
GCHQ
RICHARD J. ALDRICH
BARTON GELLMAN
DARK MIRROR
EDWARD SNOWDEN AND THE SURVEILLANCE STATE
BH
Gynaecology


BARTON GELLMAN
DARK MIRROR
EDWARD SNOWDEN AND THE SURVEILLANCE STATE
BH
GCHQ
RICHARD J. ALDRICH
THE PUZZ PALA
JAMES BAM
Gynaecology
Oats
Abraham
ÅRHUNDRADETS STÖRSTA SPIONKUPP
BORIS PROJEKTET
Sixten Svensson
BORIS HAGELIN STOP BORN HADSCHIKENT RUSSIA STOP JULY EIGHTEEN NINETY TWO STOP
NSA OCH ETT SVENSKT SNILLE LURADE EN HEL VÄRLD
CAROLINA
The Shadow Factory
JAMES BAMFORD
I ALLMÄNHETENS TJÄNST
EDWARD SNOWDEN
NO PLACE TO HIDE
GLENN GREENWALD
Michael Fredholm
UNDERRÄTTELSETJÄNSTENS VILLKOR
Pär Ström
Övervakad
Elektroniska fotspår och snokarsamhället



~~TOP SECRET~~

REPORT OF VISIT

TO

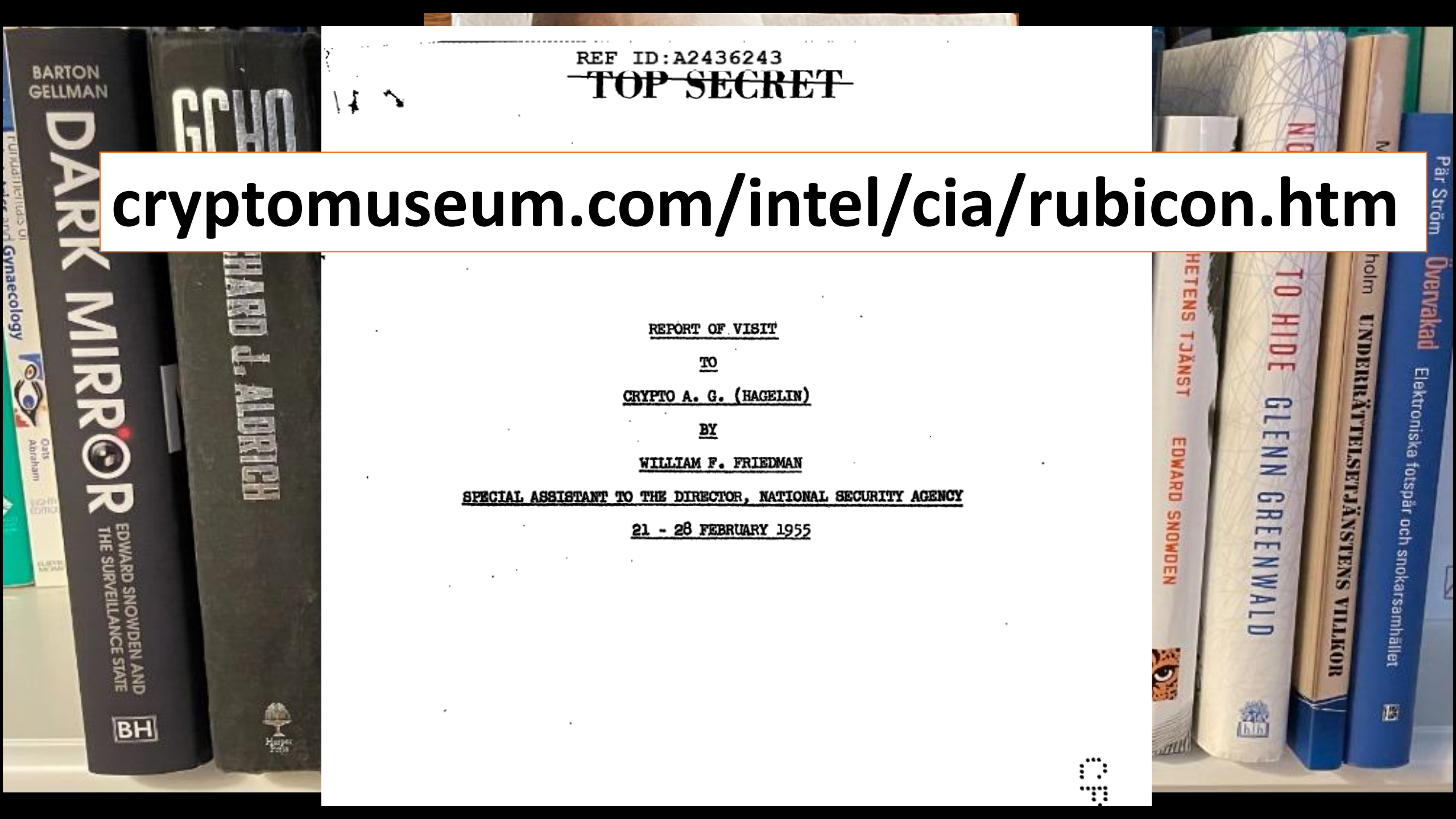
CRYPTO A. G. (HAGELIN)

BY

WILLIAM F. FRIEDMAN

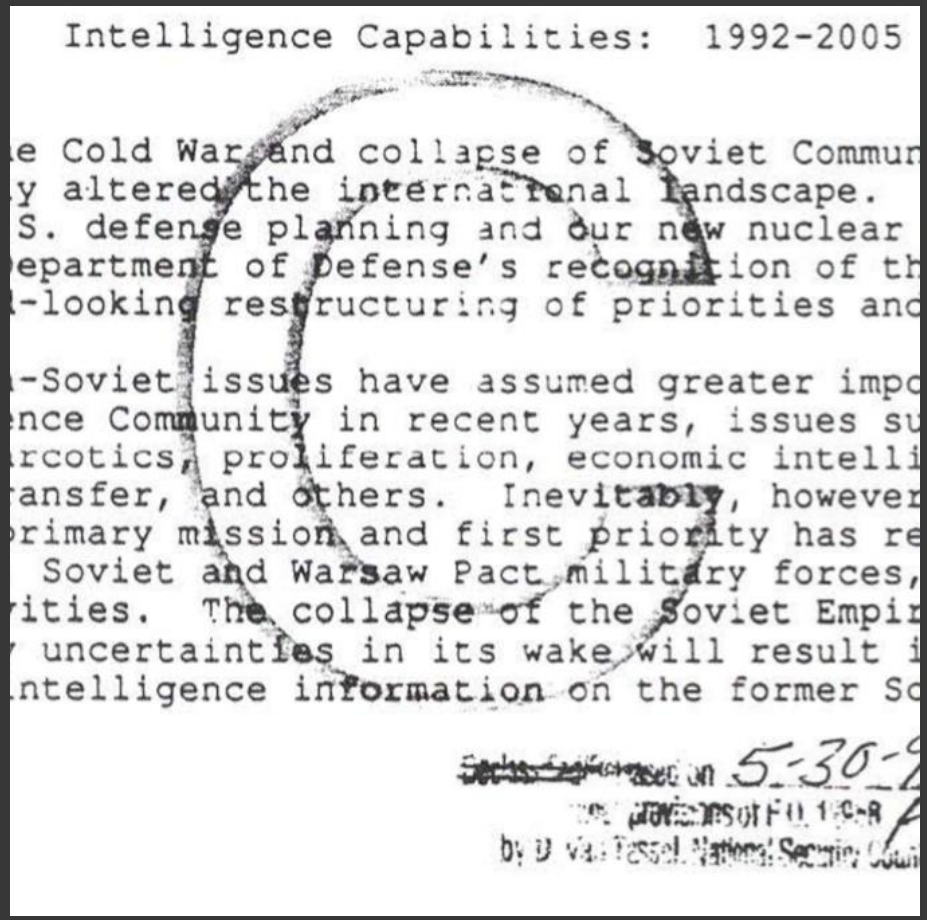
SPECIAL ASSISTANT TO THE DIRECTOR, NATIONAL SECURITY AGENCY

21 - 28 FEBRUARY 1955


BARTON GELLMAN
DARK MIRROR
EDWARD SNOWDEN AND THE SURVEILLANCE STATE
BH
REF ID:A2436243
TOP SECRET
REPORT OF VISIT
TO
CRYPTO A. G. (HAGELIN)
BY
WILLIAM F. FRIEDMAN
SPECIAL ASSISTANT TO THE DIRECTOR, NATIONAL SECURITY AGENCY
21 - 28 FEBRUARY 1955
cryptomuseum.com/intel/cia/rubicon.htm
EDWARD SNOWDEN
TO HIDE GLENN GREENWALD
UNDERRÄTTELSETJÄNSTENS VILLKOR
Pär Ström
Övervakad
Elektroniska fotspår och snokarsamhället

Economic espionage

Background and history



Intelligence Capabilities: 1992-2005

e Cold War and collapse of Soviet Commun
y altered the international landscape.
S. defense planning and our new nuclear
epartment of Defense's recognition of th
-looking restructuring of priorities and

-Soviet issues have assumed greater impo
nce Community in recent years, issues su
rcotics, proliferation, economic intelli
ansfer, and others. Inevitably, however
rimary mission and first priority has re
Soviet and Warsaw Pact military forces,
ities. The collapse of the Soviet Empir
uncertainties in its wake will result i
ntelligence information on the former So

FISA 702

Lagen och inhämtning

CATRY consulting

BLARNEY AT A GLANCE

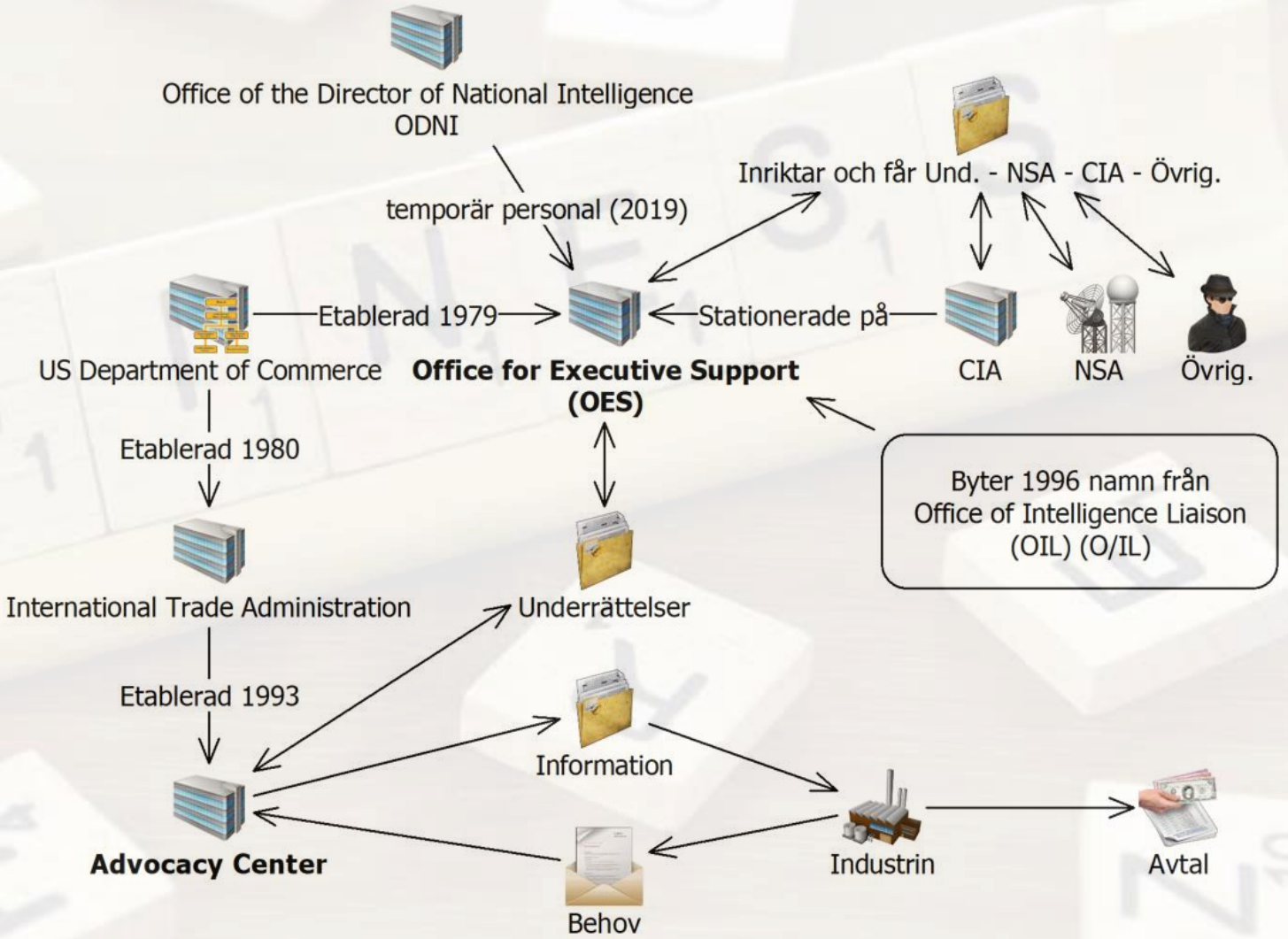
Why: Started in 1978 to provide FISA authorized access to communications of foreign establishments, agents of foreign powers, and terrorists

External Customers (Who)	Information Requirements (What)	Collection Access and Techniques (How)
Department of State	Counter Proliferation	DNI Strong Selectors
Central Intelligence Agency	Counter Terrorism	DNR Strong Selectors
United States UN Mission	Diplomatic	DNI Circuits
White House	Economic	DNR Circuits
Defense Intelligence Agency	Military	Mobile Wireless
National Counterterrorism Center	Political/Intention of Nations	
2nd Party-GBR, NZL, CAN, AUS		
Office of Director of National Intelligence		
Joint Chiefs of Staff		
Department of Homeland Security		
Office of Secretary of Defense		
North Atlantic Treaty Organization		
Military Commands (Army, EUCOM)		

Partnerships (Where)	Legal Authorities (Approvals)
NSA - SSO, TAO, NTOC, CES, A&P...	NSA FISA
CIA	CT FBI FISA
FBI – Headquarters, NY, and DC	FISA Amendment Act (FAA)
FBI – Engineering Research Facility	CI FBI FISA
DOJ	BR FISA
Commercial Providers	PR/TT FISA

Ekonomiskt spionage - USA

- Carter Administration, 1977–1981
  - Foreign Intelligence Surveillance Act, 1978
  - Office of Intelligence Liaison, 1979
- Bush Administration, 1989-1993
  - The end of the Cold War, ca:1989-91
  - The Advocacy Center, 1993
- Clinton Administration, 1993-2000
  - Office for Executive Support, 1996



Ekonomiskt spionage

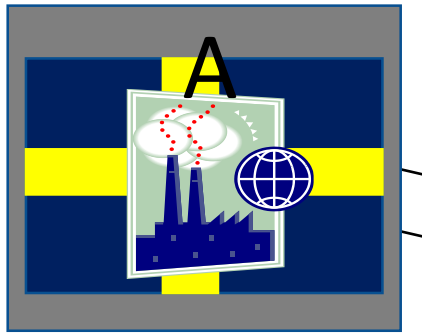
Mission Statement

Our mission is to coordinate U.S. Government resources and authority in order to level the playing field on behalf of U.S. business interests as they compete against foreign firms for specific international contracts or other U.S. export opportunities. In doing so, the Advocacy Center helps create and retain U.S. jobs through exports.

WE ACCELERATE AND FACILITATE BUSINESS WITH SWEDEN

Business Sweden facilitates and promotes the growth of Swedish companies abroad and investment opportunities for foreign companies in Sweden.

Business Sweden's aim is to strengthen and promote Sweden as an attractive, innovative and competitive business partner. We support Swedish companies in reaching export markets and identify business opportunities for small and medium-sized enterprises to grow internationally.



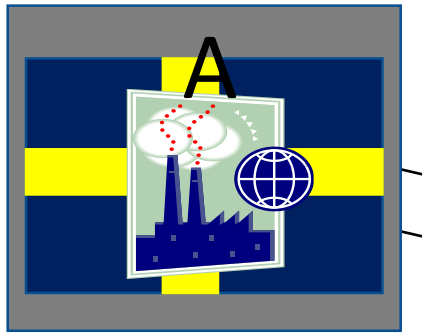
Our aim is also to facilitate for foreign companies to invest in Sweden. We connect international companies with business opportunities in Sweden - whether the interest is to gain access to the market or world class R&D and innovation clusters.

WE ACCELERATE AND FACILITATE BUSINESS WITH SWEDEN

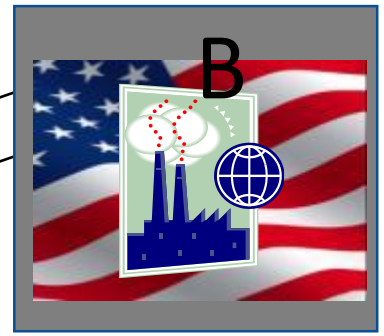
Business Sweden facilitates and promotes the growth of Swedish
opportur

Business Sv
attractive, in wedish
companies nities for
small and m

Our aim is a . We
connect inte en -
whether the interest is to gain access to the market or world class R&D and innovation clusters.



Office for Executive Support (OES)



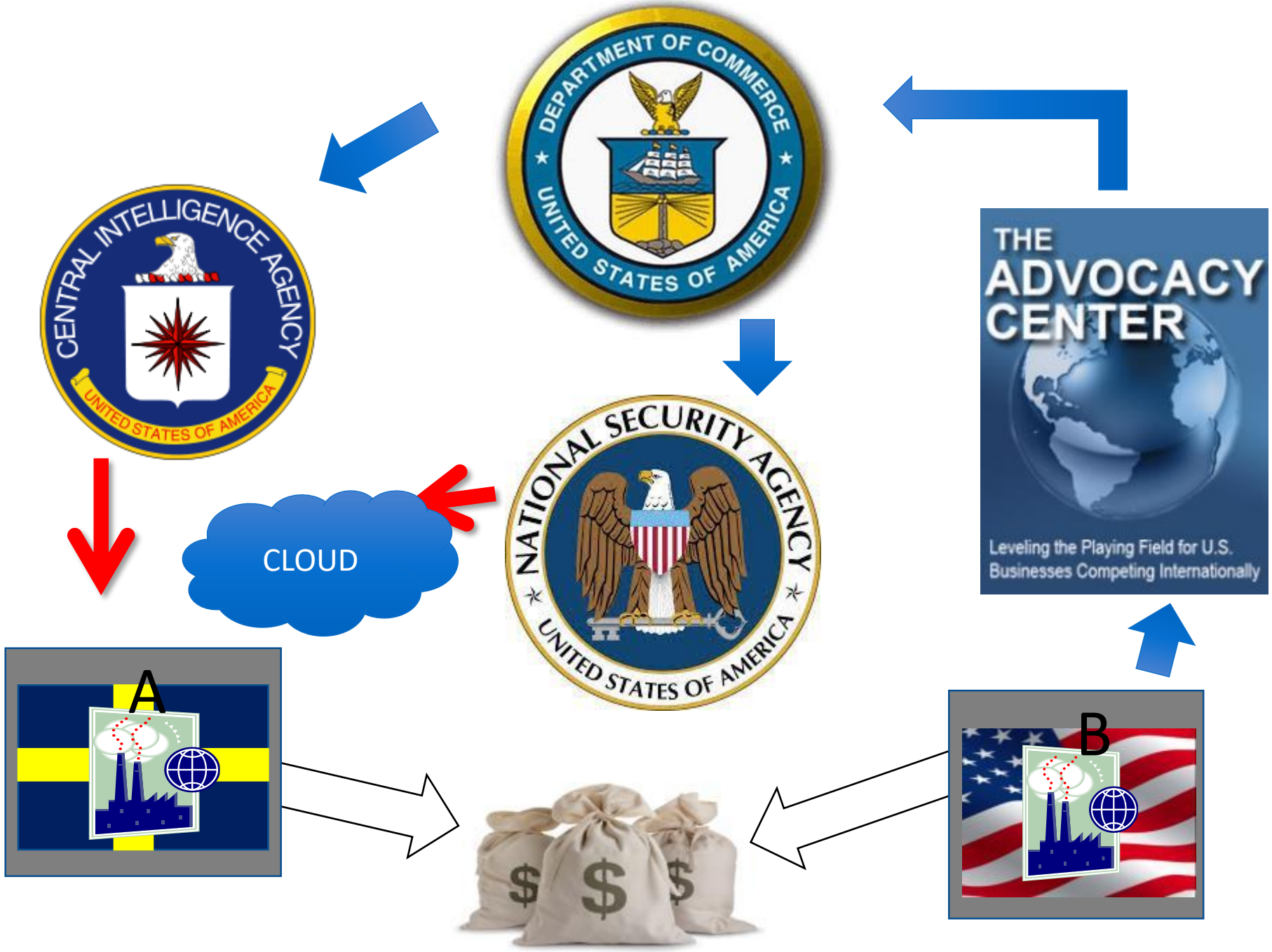
Office for Executive Support (OES)

CATRY consulting

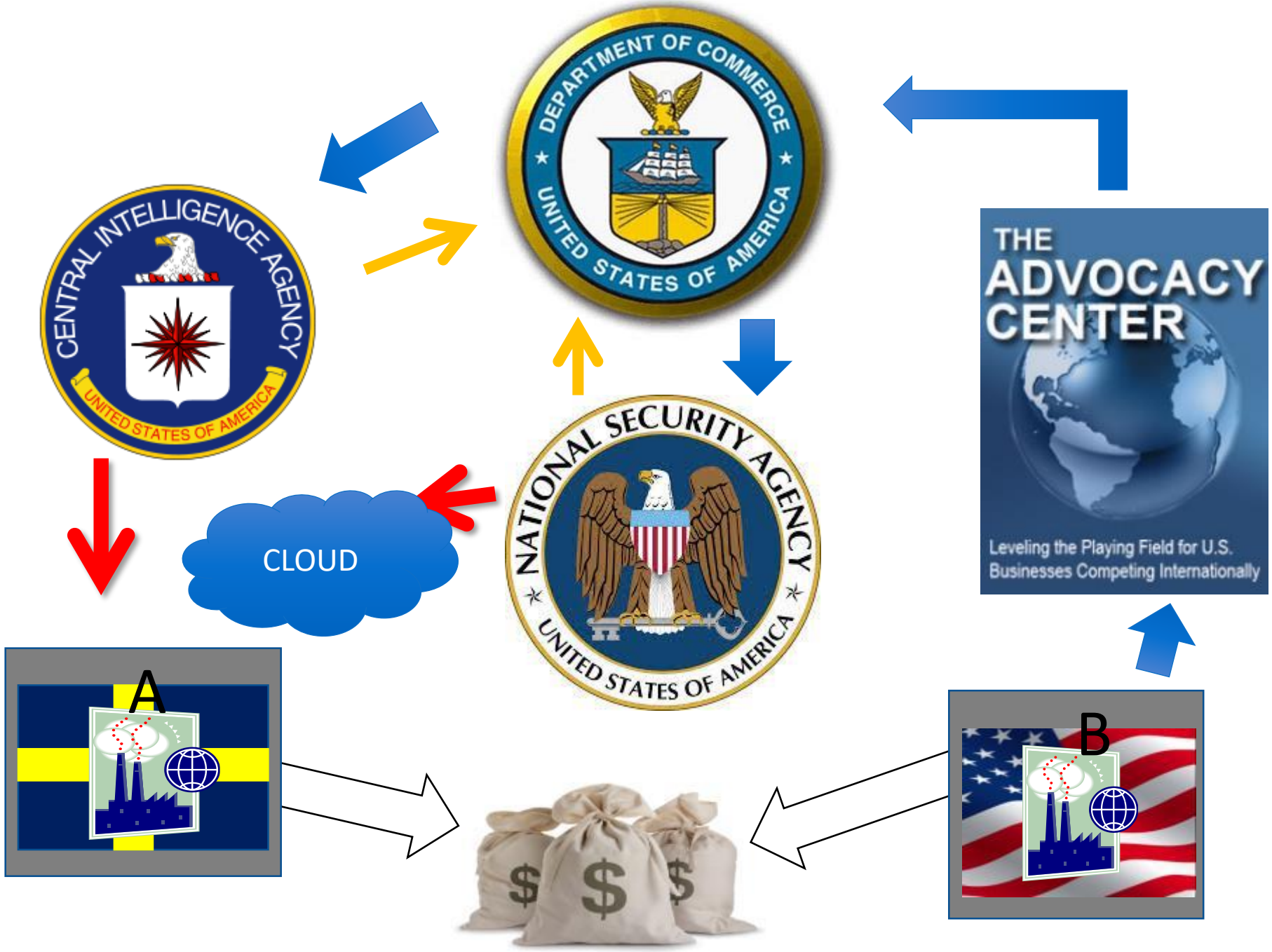
Office for Executive Support (OES)

CATRY consulting

Office for Executive Support (OES)



Office for Executive Support (OES)

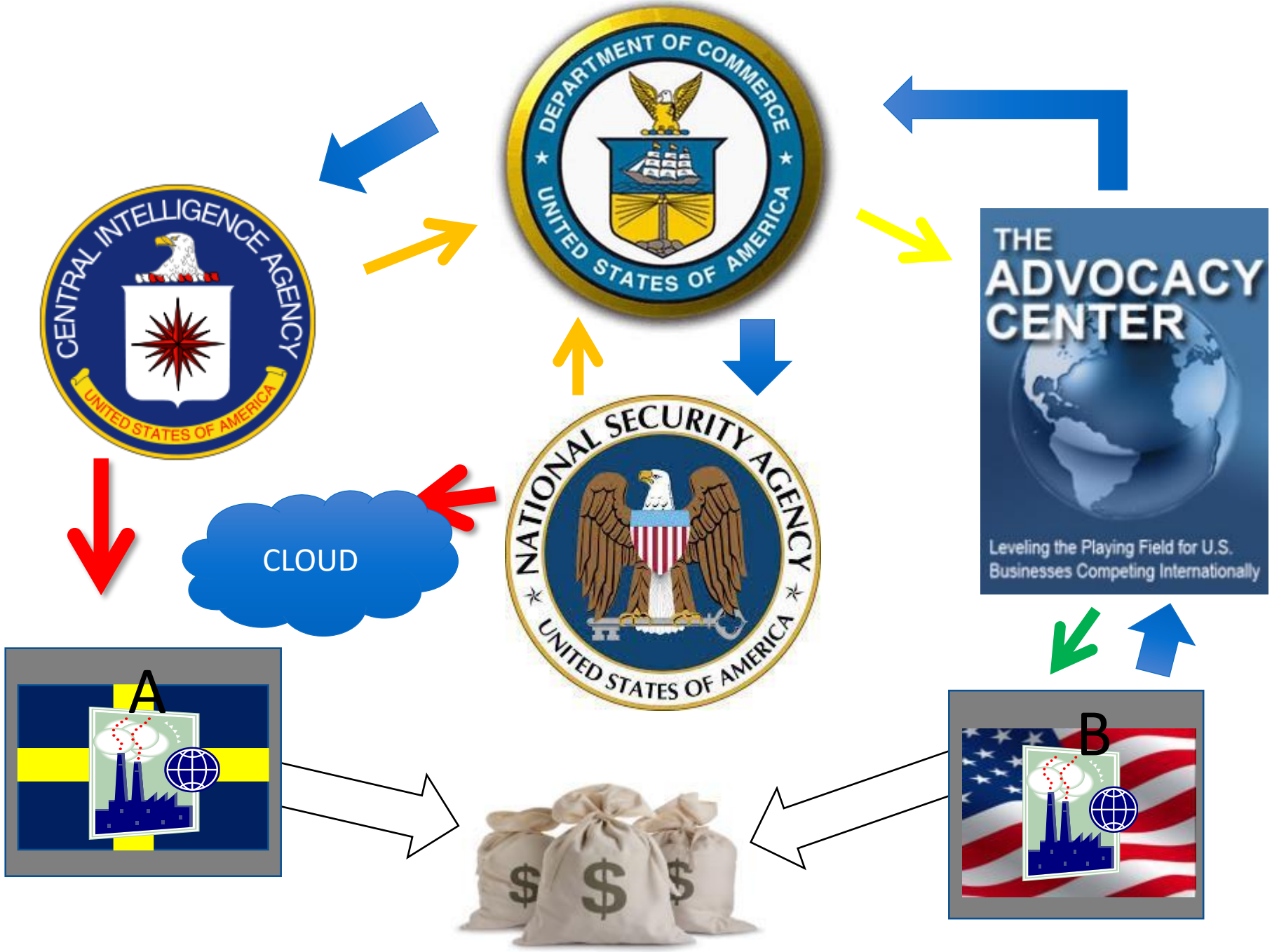


CATRY consulting

Office for Executive Support (OES)

CATRY consulting

Office for Executive Support (OES)



Ekonomiskt spionage – USA – Danmark - Sverige

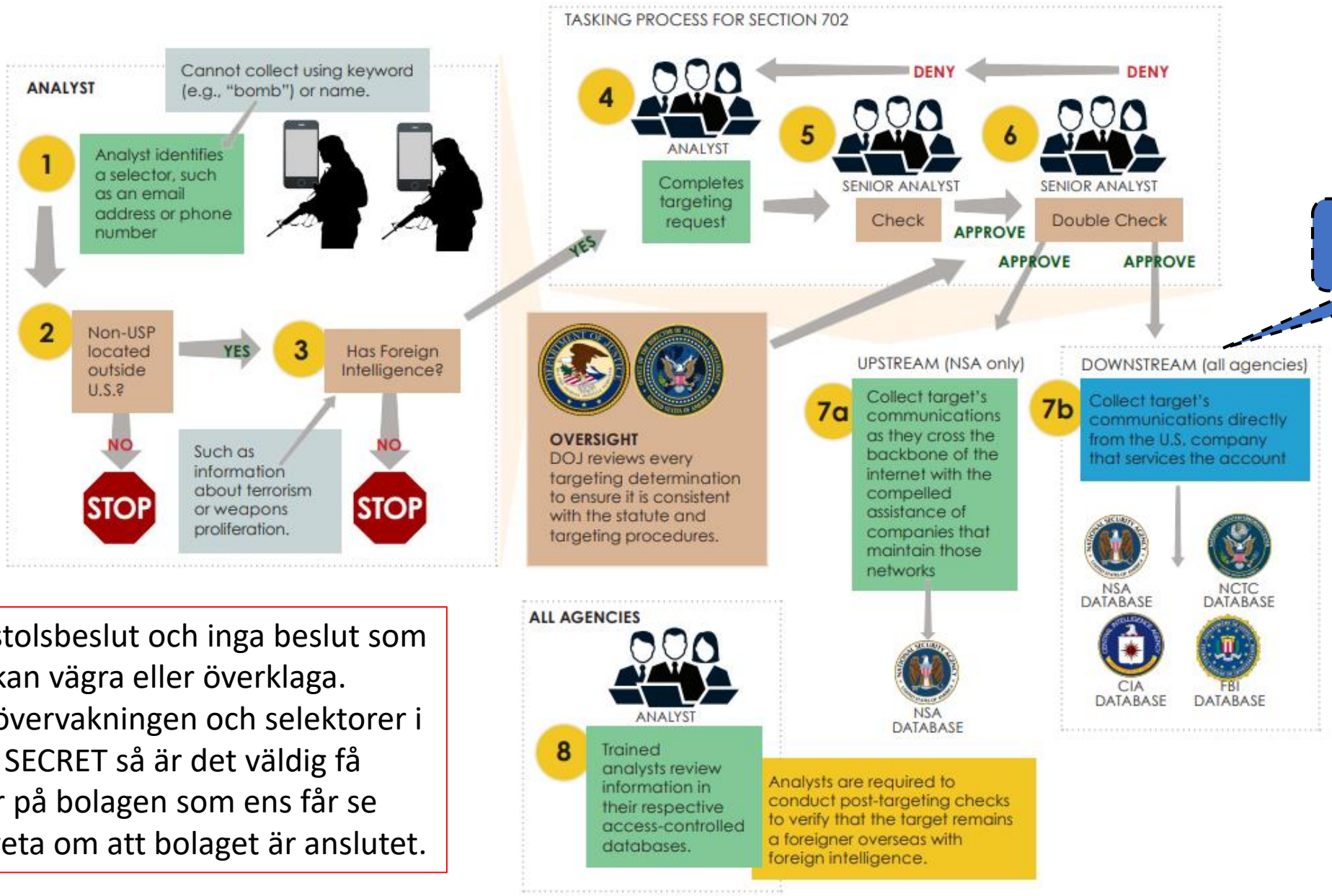
Källor till DR: USA bedrev spionage mot Saab – med hjälp av danska underättelsetjänsten

UPPDATERAD 18 NOVEMBER 2020 PUBLICERAD 14 NOVEMBER 2020

Den amerikanska underrättelsetjänsten NSA bedrev spionage mot svensk och dansk försvarsindustri från en bas i Danmark. Det avslöjar Danmarks Radio som talat med flera källor med insyn i en pågående avlyssningsskandal inom danska motsvarigheten till FRA, Forsvarets Efterretningstjeneste (FE).

SECTION 702: THE PROCESS

HOW DOES THE IC COLLECT UNDER SECTION 702?



Inga domstolsbeslut och inga beslut som ett bolag kan vägra eller överklaga. Eftersom övervakningen och selektorer i sig är TOP SECRET så är det väldig få människor på bolagen som ens får se eller ens veta om att bolaget är anslutet.

SECTION 702: THE PROCESS

HOW IS THE PROGRAM APPROVED?

The Attorney General and Director of National Intelligence submit to the Foreign Intelligence Surveillance Court (FISC) certifications that specify categories of foreign intelligence that the IC can use Section 702 to collect. Such certifications may be effective for up to one year and must be resubmitted annually.

Certifications

- The AG and DNI also submit:
  - The rules designed to ensure that the IC only uses Section 702 to target foreign persons located outside the U.S. to acquire foreign intelligence information (known as targeting procedures); and
  - The rules designed to safeguard any U.S. person information incidentally acquired through Section 702 (known as minimization procedures).

The FISC reviews the certifications and these procedures annually to ensure they comply with both FISA and the Fourth Amendment, taking into account how the program has functioned, including any compliance incidents.

Order

The FISC must issue a written opinion explaining its reasoning.

Only upon FISC approval of the certifications, including the targeting and minimization procedures, the AG and DNI can issue written directives compelling U.S. electronic communication service providers to assist with collection against authorized Section 702 targets.

SECTION 702: THE PROCESS

TOP SECRET//NOFORN

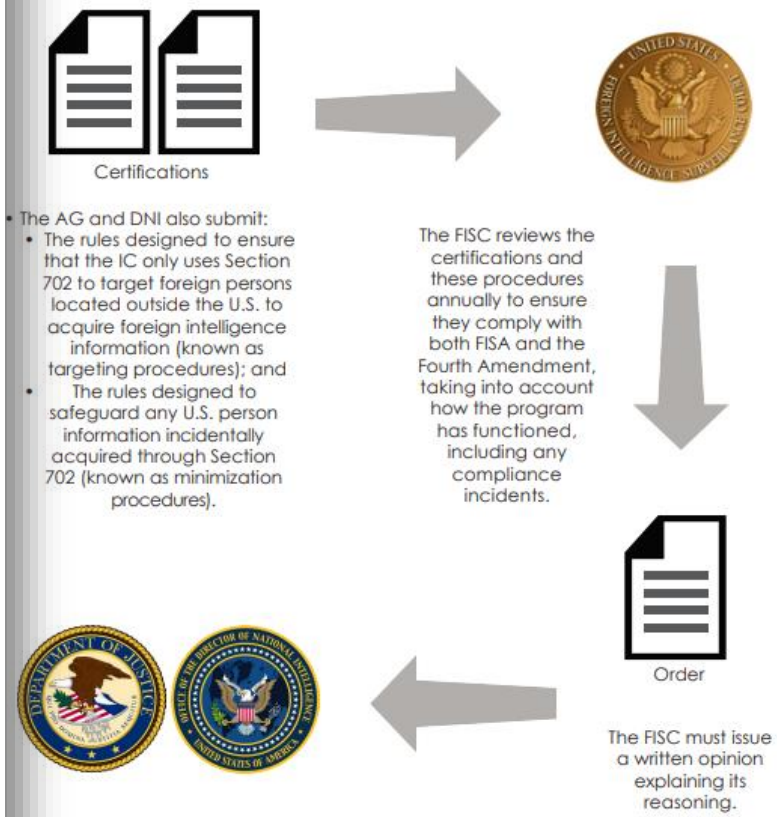
EXHIBIT F

IN THE MATTER OF FOREIGN GOVERNMENTS, FOREIGN FACTIONS, FOREIGN ENTITIES, AND FOREIGN-BASED POLITICAL ORGANIZATIONS

DNI/AG 702(g) Certification 2010-A

Foreign Governments or Any Components Thereof, Whether or Not Recognized by the United States (50 U.S.C. § 1801(a)(1)):

Afghanistan; Albania; Algeria; Andorra; Angola; Antigua and Barbuda; Argentina; Armenia; Austria; Azerbaijan; Bahamas; Bahrain; Bangladesh; Barbados; Belarus; Belgium; Belize; Benin; Bhutan; Bolivia; Bosnia and Herzegovina; Botswana; Brazil; Brunei; Bulgaria; Burkina Faso; Burma (Myanmar); Burundi; Cambodia; Cameroon; Cape Verde; Central African Republic; Chad; Chile; China; Colombia; Comoros; Congo, Democratic Republic; Congo, Republic; Costa Rica; Cote d'Ivoire; Croatia; Cuba; Cyprus; Czech Republic; Denmark; Djibouti; Dominica; Dominican Republic; East Timor (Timor-Leste); Ecuador; Egypt; El Salvador; Equatorial Guinea; Eritrea; Estonia; Ethiopia; Fiji; Finland; France; Gabon; Gambia; Georgia; Germany; Ghana; Greece; Grenada; Guatemala; Guinea; Guinea-Bissau; Guyana; Haiti; Honduras; Hungary; Iceland; India; Indonesia; Iran; Iraq; Ireland; Israel; Italy; Jamaica; Japan; Jordan; Kazakhstan; Kenya; Kiribati; Korea, Democratic Peoples Republic of (DPRK); Korea, Republic of (ROK); Kosovo; Kuwait; Kyrgyzstan; Laos; Latvia; Lebanon; Lesotho; Liberia; Libya; Liechtenstein; Lithuania; Luxembourg; Macedonia; Madagascar; Malawi; Malaysia; Maldives; Mali; Malta; Marshall Islands; Mauritania; Mauritius; Mexico; Micronesia; Moldova; Monaco; Mongolia; Montenegro; Morocco; Mozambique; Namibia; Nauru; Nepal; Netherlands; Nicaragua; Niger; Nigeria; Norway; Oman; Pakistan; Palau; Panama; Papua New Guinea; Paraguay; Peru; Philippines; Poland; Portugal; Qatar; Romania; Russia; Rwanda; Saint Kitts and Nevis; Saint Lucia; Saint Vincent and the Grenadines; Samoa; San Marino; Sao Tome and Principe; Saudi Arabia; Senegal; Serbia; Seychelles; Sierra Leone; Singapore; Slovakia; Slovenia; Solomon Islands; Somalia; South Africa; Spain; Sri Lanka; Sudan; Suriname; Swaziland; Sweden; Switzerland; Syria; Taiwan; Tajikistan; Tanzania; Thailand; Togo; Tonga; Trinidad and Tobago; Tunisia; Turkey; Turkmenistan; Tuvalu; Uganda; Ukraine; United Arab Emirates; Uruguay; Uzbekistan; Vanuatu; Vatican City (Holy See); Venezuela; Vietnam; Western Sahara; Yemen; Zambia; Zimbabwe. (TS//NF)



SECTION 702: THE PROCESS

TOP SECRET//NOFORN

EXHIBIT F

IN THE MATTER OF FOREIGN GOVERNMENTS, FOREIGN FACTIONS, FOREIGN ENTITIES, AND FOREIGN-BASED POLITICAL ORGANIZATIONS

DNI/AG 702(g) Certification 2010-A

Foreign Governments or Any Components Thereof, Whether or Not Recognized by the United States (50 U.S.C. § 1801(a)(1)):

Afghanistan; Albania; Algeria; Andorra; Angola; Antigua and Barbuda; Argentina; Armenia; Austria; Azerbaijan; Bahamas; Bahrain; Bangladesh; Barbados; Belarus; Belgium; Belize; Benin; Bhutan; Bolivia; Bosnia and Herzegovina; Botswana; Brazil; Brunei; Bulgaria; Burkina Faso; Burma (Myanmar); Burundi; Cambodia; Cameroon; Cape Verde; Central African Republic; Chad; Chile; China; Colombia; Comoros; Congo, Democratic Republic; Congo, Republic; Costa Rica; Cote d'Ivoire; Croatia; Cuba; Cyprus; Czech Republic; Denmark; Djibouti; Dominica; Dominican Republic; East Timor (Timor-Leste); Ecuador; Egypt; El Salvador; Equatorial Guinea; Eritrea; Estonia; Ethiopia; Fiji; Finland; France; Gabon; Gambia; Georgia; Germany; Ghana; Greece; Grenada; Guatemala; Guinea; Guinea-Bissau; Guyana; Haiti; Honduras; Hungary; Iceland; India; Indonesia; Iran; Iraq; Ireland; Israel; Italy; Jamaica; Japan; Jordan; Kazakhstan; Kenya; Kiribati; Korea, Democratic Peoples Republic of (DPRK); Korea, Republic of (ROK); Kosovo; Kuwait; Kyrgyzstan; Laos; Latvia; Lebanon; Lesotho; Liberia; Libya; Liechtenstein; Lithuania; Luxembourg; Macedonia; Madagascar; Malawi; Malaysia; Maldives; Mali; Malta; Marshall Islands; Mauritania; Mauritius; Mexico; Micronesia; Moldova; Monaco; Mongolia; Montenegro; Morocco; Mozambique; Namibia; Nauru; Nepal; Netherlands; Nicaragua; Niger; Nigeria; Norway; Oman; Pakistan; Palau; Panama; Papua New Guinea; Paraguay; Peru; Philippines; Poland; Portugal; Qatar; Romania; Russia; Rwanda; Saint Kitts and Nevis; Saint Lucia; Saint Vincent and the Grenadines; Samoa; San Marino; Sao Tome and Principe; Saudi Arabia; Senegal; Serbia; Seychelles; Sierra Leone; Singapore; Slovakia; Slovenia; Solomon Islands; Somalia; South Africa; Spain; Sri Lanka; Sudan; Suriname; Swaziland; Sweden; Switzerland; Syria; Taiwan; Tajikistan; Tanzania; Thailand; Togo; Tonga; Trinidad and Tobago; Tunisia; Turkey; Turkmenistan; Tuvalu; Uganda; Ukraine; United Arab Emirates; Uruguay; Uzbekistan; Vanuatu; Vatican City (Holy See); Venezuela; Vietnam; Western Sahara; Yemen; Zambia; Zimbabwe. (TS//NF)

Certifications

- The AG and DNI also submit:
  - The rules designed to ensure that the IC only uses Section 70
  - to
  - s
  - a 70

The FISC reviews the certifications and

TOP SECRET//NOFORN

Entities Openly Acknowledged by a Foreign Government or Governments to be Directed and Controlled by Such Foreign Government or Governments (50 U.S.C. § 1801(a)(3)):

United Nations; International Atomic Energy Agency; World Bank Group; International Monetary Fund; Inter-American Development Bank; European Central Bank; European Union; African Union; Organization of the Petroleum Exporting Countries; African Development Bank; Asian Development Bank; Bank for International Settlements; European Bank for Reconstruction and Development; Financial Action Task Force; Gas Producers' Forum; Islamic Development Bank; League of Arab States; Mercosur. (TS//NF)

a written opinion explaining its reasoning.

CATRY consulting

SECTION 702: THE PROCESS

HOW IS THE PROGRAM APPROVED?

The Attorney General and Director of National Intelligence submit to the Foreign Intelligence Surveillance Court (FISC) certifications that specify categories of foreign intelligence that the IC can use Section 702 to collect. Such certifications may be effective for up to one year and must be resubmitted annually.

Certifications

- The AG and DNI also submit:
  - The rules designed to ensure that the IC only uses Section 702 to target foreign persons located outside the U.S. to acquire foreign intelligence information (known as targeting procedures); and
  - The rules designed to safeguard any U.S. person information incidentally acquired through Section 702 (known as minimization procedures).

The FISC reviews the certifications and these procedures annually to ensure they comply with both FISA and the Fourth Amendment, taking into account how the program has functioned, including any compliance incidents.

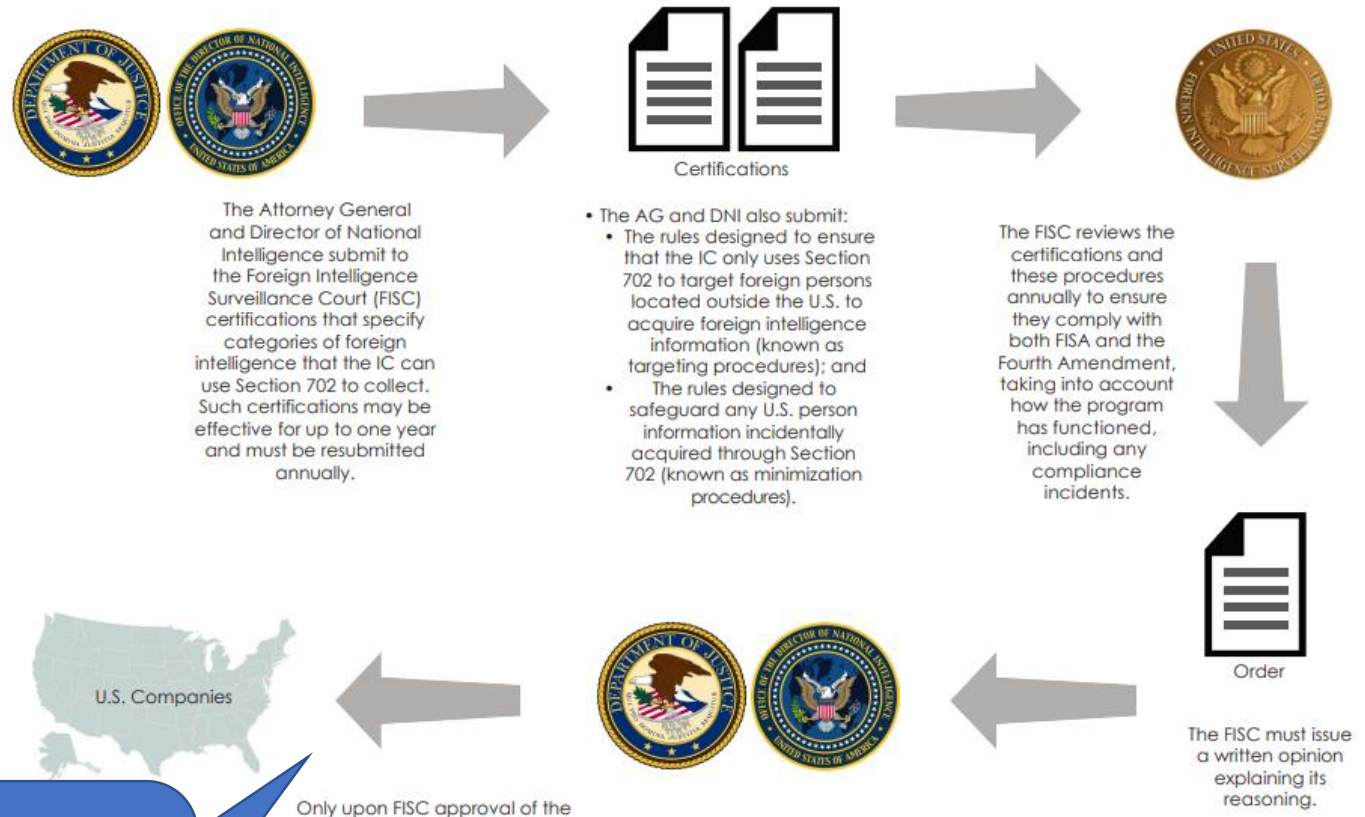
Order

The FISC must issue a written opinion explaining its reasoning.

Only upon FISC approval of the certifications, including the targeting and minimization procedures, the AG and DNI can issue written directives compelling U.S. electronic communication service providers to assist with collection against authorized Section 702 targets.

SECTION 702: THE PROCESS

HOW IS THE PROGRAM APPROVED?



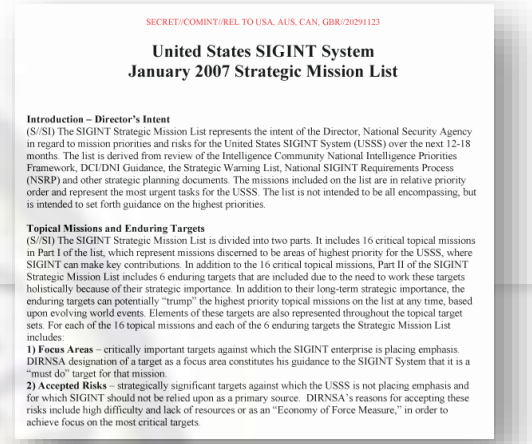
Yahoo begär att FISA –domstolen FISC ska avslöja en incident från 2008 där de vägrade följa NSA -övervakning tills domstolen krävde att de skulle lämna kunddata.

NSA director defends plan to maintain 'backdoors' into technology companies

- Rogers admitted that concerns about US government infiltration of US companies' data represented a business risk for US companies, but he suggested that the greater threat was from cyber-attacks.
- "I think it's a very valid concern to say 'Look, are we losing US market segment here?'" Rogers said. "What's the economic impact of this? I just think, between a combination of technology, legality and policy, we can get to a better place than we are now."

www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies

United States SIGINT System
January 2007 Strategic Mission List



SECRET//COMINT//REL TO USA, AUS, CAN, GBR//20291123

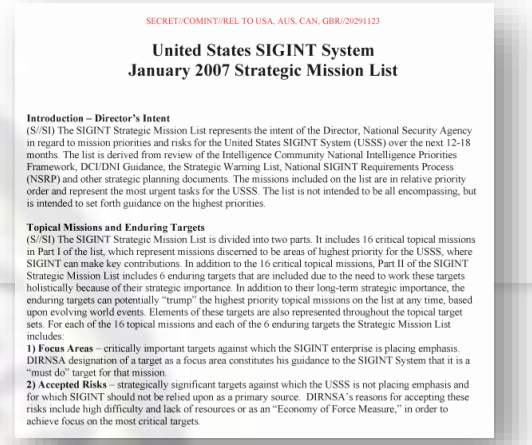
United States SIGINT System
January 2007 Strategic Mission List

Introduction – Director's Intent
(S//SI) The SIGINT Strategic Mission List represents the intent of the Director, National Security Agency in regard to mission priorities and risks for the United States SIGINT System (USSS) over the next 12-18 months. The list is derived from review of the Intelligence Community National Intelligence Priorities Framework, DCI/DNI Guidance, the Strategic Warning List, National SIGINT Requirements Process (NSRP) and other strategic planning documents. The missions included on the list are in relative priority order and represent the most urgent tasks for the USSS. The list is not intended to be all encompassing, but is intended to set forth guidance on the highest priorities.

Topical Missions and Enduring Targets
(S//SI) The SIGINT Strategic Mission List is divided into two parts. It includes 16 critical topical missions in Part I of the list, which represent missions discerned to be areas of highest priority for the USSS, where SIGINT can make key contributions. In addition to the 16 critical topical missions, Part II of the SIGINT Strategic Mission List includes 6 enduring targets that are included due to the need to work these targets holistically because of their strategic importance. In addition to their long-term strategic importance, the enduring targets can potentially "trump" the highest priority topical missions on the list at any time, based upon evolving world events. Elements of these targets are also represented throughout the topical target sets. For each of the 16 topical missions and each of the 6 enduring targets the Strategic Mission List includes:
1) Focus Areas – critically important targets against which the SIGINT enterprise is placing emphasis. DIRNSA designation of a target as a focus area constitutes his guidance to the SIGINT System that it is a "must do" target for that mission.
2) Accepted Risks – strategically significant targets against which the USSS is not placing emphasis and for which SIGINT should not be relied upon as a primary source. DIRNSA's reasons for accepting these risks include high difficulty and lack of resources or as an "Economy of Force Measure," in order to achieve focus on the most critical targets.

(S//SI) **J. MISSION: Emerging Strategic Technologies: Preventing Technological Surprise.**
Focus Areas: Critical technologies that could provide a strategic military, economic, **or political** advantage: high energy lasers, low energy lasers, advances in computing and information technology, directed energy weapons, **stealth and counter-stealth**, electronic warfare technologies, space and remote sensing, electro-optics, nanotechnologies, energetic materials. The emerging strategic technology threat is expected to come mainly from Russia, China, India, Japan, Germany, France, Korea, Israel, Singapore, and Sweden.
Accepted Risks: Technological advances and/or basic S&T development on a global basis elsewhere.

United States SIGINT System
January 2007 Strategic Mission List



SECRET//COMINT//REL TO USA, AUS, CAN, GBR//20291123

United States SIGINT System
January 2007 Strategic Mission List

Introduction – Director's Intent
(S//SI) The SIGINT Strategic Mission List represents the intent of the Director, National Security Agency in regard to mission priorities and risks for the United States SIGINT System (USSS) over the next 12-18 months. The list is derived from review of the Intelligence Community National Intelligence Priorities Framework, DCI/DNI Guidance, the Strategic Warning List, National SIGINT Requirements Process (NSRP) and other strategic planning documents. The missions included on the list are in relative priority order and represent the most urgent tasks for the USSS. The list is not intended to be all encompassing, but is intended to set forth guidance on the highest priorities.

Topical Missions and Enduring Targets
(S//SI) The SIGINT Strategic Mission List is divided into two parts. It includes 16 critical topical missions in Part I of the list, which represent missions discerned to be areas of highest priority for the USSS, where SIGINT can make key contributions. In addition to the 16 critical topical missions, Part II of the SIGINT Strategic Mission List includes 6 enduring targets that are included due to the need to work these targets holistically because of their strategic importance. In addition to their long-term strategic importance, the enduring targets can potentially "trump" the highest priority topical missions on the list at any time, based upon evolving world events. Elements of these targets are also represented throughout the topical target sets. For each of the 16 topical missions and each of the 6 enduring targets the Strategic Mission List includes:
1) Focus Areas – critically important targets against which the SIGINT enterprise is placing emphasis. DIRNSA designation of a target as a focus area constitutes his guidance to the SIGINT System that it is a "must do" target for that mission.
2) Accepted Risks – strategically significant targets against which the USSS is not placing emphasis and for which SIGINT should not be relied upon as a primary source. DIRNSA's reasons for accepting these risks include high difficulty and lack of resources or as an "Economy of Force Measure," in order to achieve focus on the most critical targets.

(S//REL USA, AUS, CAN, GBR, NZL) **H. MISSION: Information Operations: Mastering Cyberspace and Preventing an Attack on U.S. Critical Information Systems.**

Focus Areas:

a. (S//SI) Enabling Computer Network Defense (CND): Provide cyber threat warning, detection, characterization, and mitigation services for U.S. and allied computer network operators: Named Intrusion Sets (Including, but not limited to: Gadget Hiss, Seed Sphere/Byzantine Trace, Makers Mark, Byzantine Candor), New intrusions.

b. (S//REL USA, AUS, CAN, GBR, NZL) Enabling Computer Network Attack (CNA): Deliver intelligence, access, and dual-use capabilities in support of U.S. computer network attack objectives.

c. (S//SI) Foreign Intelligence Services' Cyber Threat Activities: Deliver intelligence on the capabilities, vulnerabilities, plans and intentions of foreign actors to conduct CNO against USG networks and those of interest to the USG. Identify what Foreign Intel Services know about USG capabilities, vulnerabilities, plans and intentions to conduct CNO: China, Russia, Iran, and al-Qa'ida.

d. (S//SI) Enabling Electronic Warfare (EW): Provide cognizance of the EM environment, signal detection/geolocation, and characterization through intelligence (ELINT, COMINT, Tech SIGINT) and other technical means to U.S. EW planners and operators: China, Russia, Iran, Iraq/Afghanistan (IED's) and North Korea.

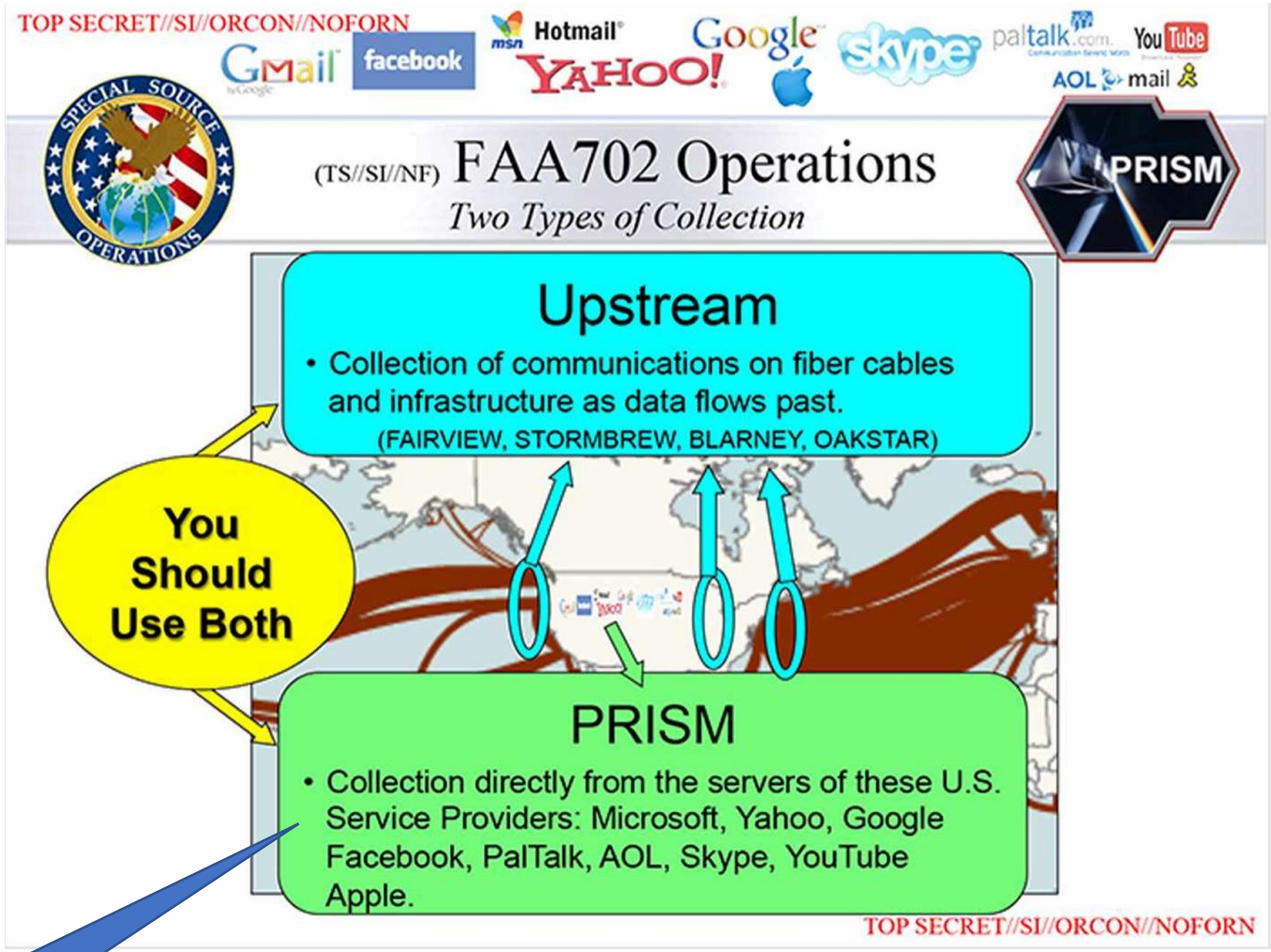
e. (S//SI) Enabling Influence Operations: Support U.S. military deception (MILDEC) and psychological operations (PSYOP), and inter-agency Strategic Communication objectives to influence target behavior and activities: Terrorist groups, China, North Korea, Iran, and Venezuela.

Accepted Risks:

a. Enabling CND: Isolated malicious activity that could pose a serious threat.
b. Enabling CNA.
c. FIS Cyber Threat: France, Israel, Cuba, India, and North Korea.
d. Enabling EW: (producers/proliferators): Sweden, Japan, Germany, Israel, and France.
e. Enabling Influence Operations: Pakistan and Russia.

FISA 702 PRISM och Upstream

FISA 702 PRISM och Upstream



Downstream

FISA 702 PRISM, Upstream och EO12333

Special Source Operations division (**SSO**)

FISA 702 PRISM, Upstream och EO12333

Microsoft
AWS
Google
Facebook

PRISM DOWNSTREAM FISA 702

Special Source Operations division (**SSO**)

FISA 702 PRISM, Upstream och EO12333

Microsoft
AWS
Google
Facebook

PRISM DOWNSTREAM FISA 702

UPSTREAM EO 12333 FISA 702

Special Source Operations division (**SSO**)

(S//SI) **J. MISSION: Emerging Strategic Technologies: Preventing Technological Surprise.**
Focus Areas: Critical technologies that could provide a strategic military, economic, **or political** advantage: high energy lasers, low energy lasers, advances in computing and information technology, directed energy weapons, **stealth and counter-stealth**, electronic warfare technologies, space and remote sensing, electro-optics, nanotechnologies, energetic materials. The emerging strategic technology threat is expected to come mainly from Russia, China, India, Japan, Germany, France, Korea, Israel, Singapore, and Sweden.
Accepted Risks: Technological advances and/or basic S&T development on a global basis elsewhere.

Källor till DR: USA bedrev spionage mot Saab – med hjälp av danska underättelsetjänsten

UPPDATERAD 18 NOVEMBER 2020 PUBLICERAD 14 NOVEMBER 2020

Den amerikanska underrättelsetjänsten NSA bedrev spionage mot svensk och dansk försvarsindustri från en bas i Danmark. Det avslöjar Danmarks Radio som talat med flera källor med insyn i en pågående avlyssningsskandal inom danska motsvarigheten till FRA, Forsvarets Efterretningstjeneste (FE).

Bland målen för amerikanska NSA:s avlyssning fanns Saab och den danska försvarskoncernen Terma. Enligt uppgifter till DR, från flera av varandra oberoende källor med insyn i granskningen av den pågående avlyssningsskandalen i Danmark, har NSA fått tillgång till fiberoptiska kablar och ett datacenter på Amager söder om Köpenhamn. Därifrån har man avlyssnat holländsk, norsk, fransk och tysk datatrafik, danska politiska institutioner och svenska försvarsintressen.

(S//REL USA, AUS, CAN, GBR, NZL) **H. MISSION: Information Operations: Mastering Cyberspace and Preventing an Attack on U.S. Critical Information Systems.**
Focus Areas:
a. (S//SI) Enabling Computer Network Defense (CND): Provide cyber threat warning, detection, characterization, and mitigation services for U.S. and allied computer network operators: Named Intrusion Sets (Including, but not limited to: Gadget Hiss, Seed Sphere/Byzantine Trace, Makers Mark, Byzantine Candor), New intrusions.
b. (S//REL USA, AUS, CAN, GBR, NZL) Enabling Computer Network Attack (CNA): Deliver intelligence, access, and dual-use capabilities in support of U.S. computer network attack objectives.
c. (S//SI) Foreign Intelligence Services' Cyber Threat Activities: Deliver intelligence on the capabilities, vulnerabilities, plans and intentions of foreign actors to conduct CNO against USG networks and those of interest to the USG. Identify what Foreign Intel Services know about USG capabilities, vulnerabilities, plans and intentions to conduct CNO: China, Russia, Iran, and al-Qa'ida.
d. (S//SI) Enabling Electronic Warfare (EW): Provide cognizance of the EM environment, signal detection/geolocation, and characterization through intelligence (ELINT, COMINT, Tech SIGINT) and other technical means to U.S. EW planners and operators: China, Russia, Iran, Iraq/Afghanistan (IED's) and North Korea.
e. (S//SI) Enabling Influence Operations: Support U.S. military deception (MILDEC) and psychological operations (PSYOP), and inter-agency Strategic Communication objectives to influence target behavior and activities: Terrorist groups, China, North Korea, Iran, and Venezuela.
Accepted Risks:
a. Enabling CND: Isolated malicious activity that could pose a serious threat.
b. Enabling CNA.
c. FIS Cyber Threat: France, Israel, Cuba, India, and North Korea.
d. Enabling EW: (producers/proliferators): Sweden, Japan, Germany, Israel, and France.
e. Enabling Influence Operations: Pakistan and Russia.

Ekonomiskt och politiskt spionage

Säkerhetspolisen

De som spionerar sid 28

Länderna som spionerar mot Sverige

Ett 15-tal länder bedriver underrättelseverksamhet och har underrättelseofficerare i Sverige. Hot, spionage, påverkansoperationer och uppköp av strategisk betydelse är några exempel på hur andra länder försöker försvaga Sverige och påverka demokratin.

Det som kännetecknar de länder som bedriver säkerhetshotande verksamhet mot Sverige är att de lägger ner pengar, personella resurser och många år på att uppnå sina säkerhetspolitiska mål. Ryssland, Kina och Iran är de länder som utgör det största underrättelsehotet.

Stefan Kristiansson
Tidigare C MUST
Sveket mot cybersäkerheten
FORES 2022

De svenska underrättelse- och säkerhetstjänsterna har under flera år varnat för att underrättelseverksamheten ökat mot vårt land. Enligt Säkerhetspolisen bedriver ett femtontal länder spioneri mot landet. Ryssland, Kina och Iran pekas ut[1]. Det är bra att man är så konkret när det gäller dessa tre aktörer och att man inte använder uttrycket ”främmande makt”. Risken är dock att fokus hamnar helt på de utpekade tre och att vi inte i tillräcklig grad skyddar oss mot de andra tolv.

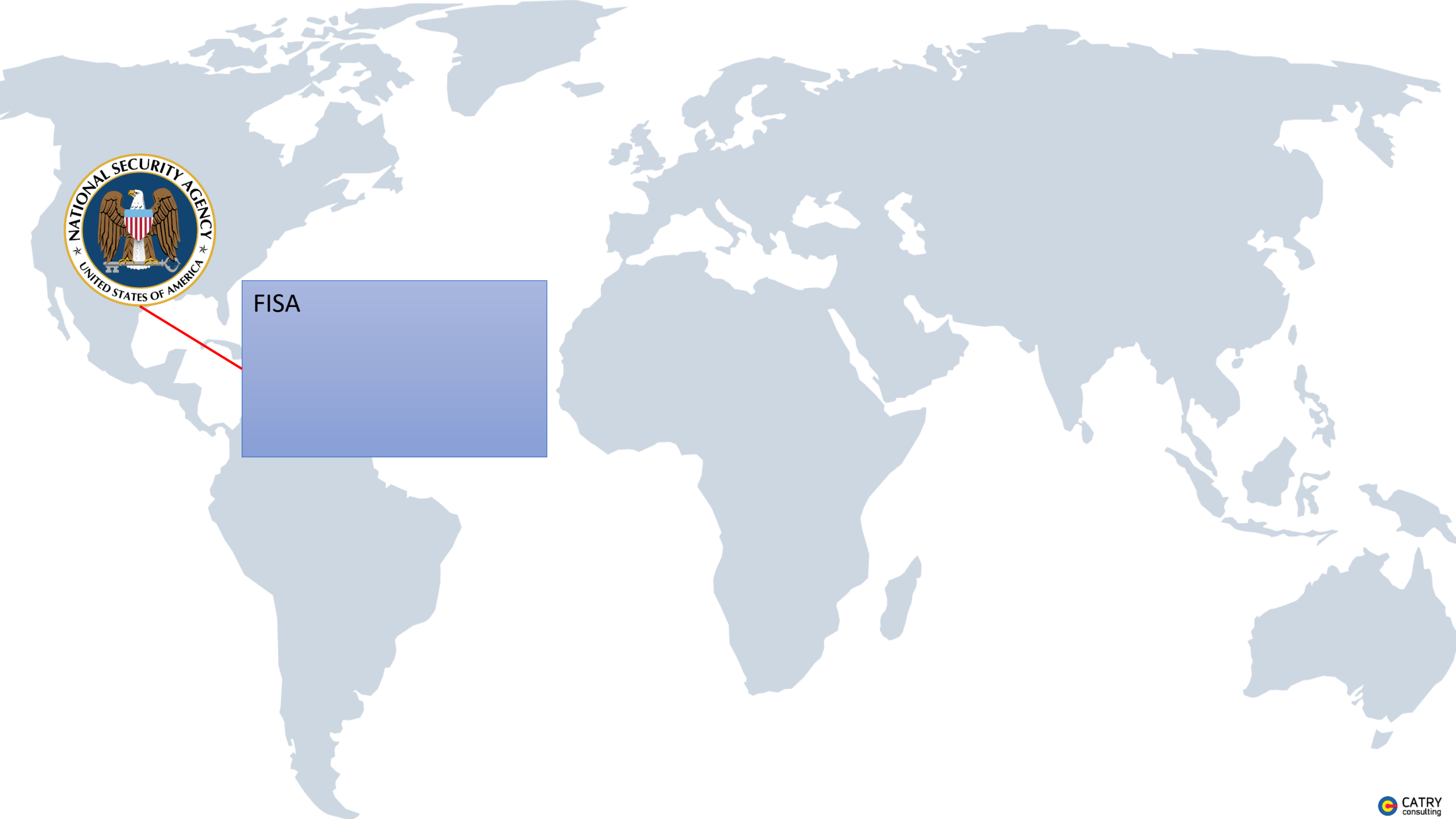
Intrång i våra informationssystem torde vara det största, mest akuta och ökande underrättelsehotet.

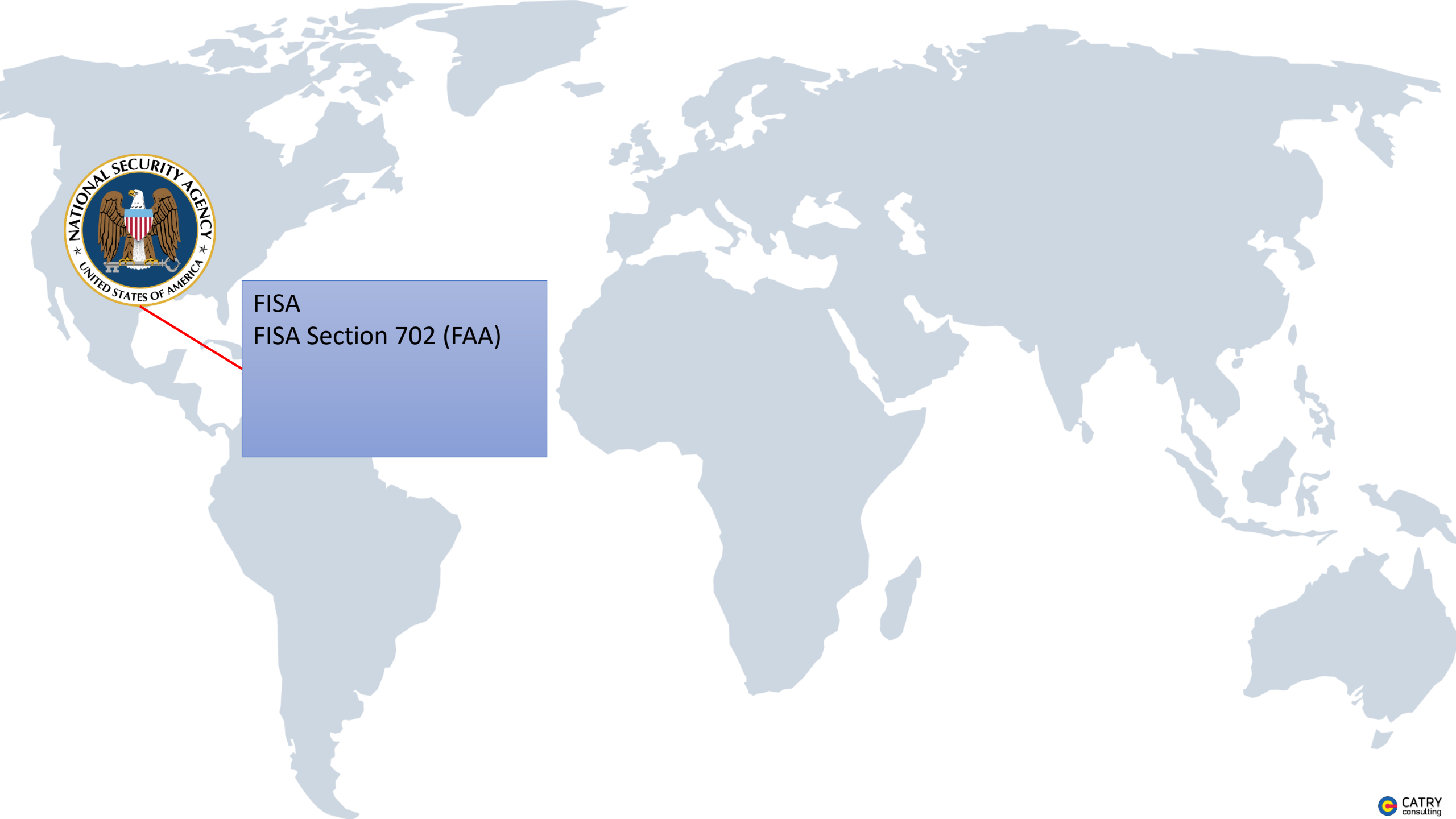
”Och så till sist … även vänner och allierade spionerar”

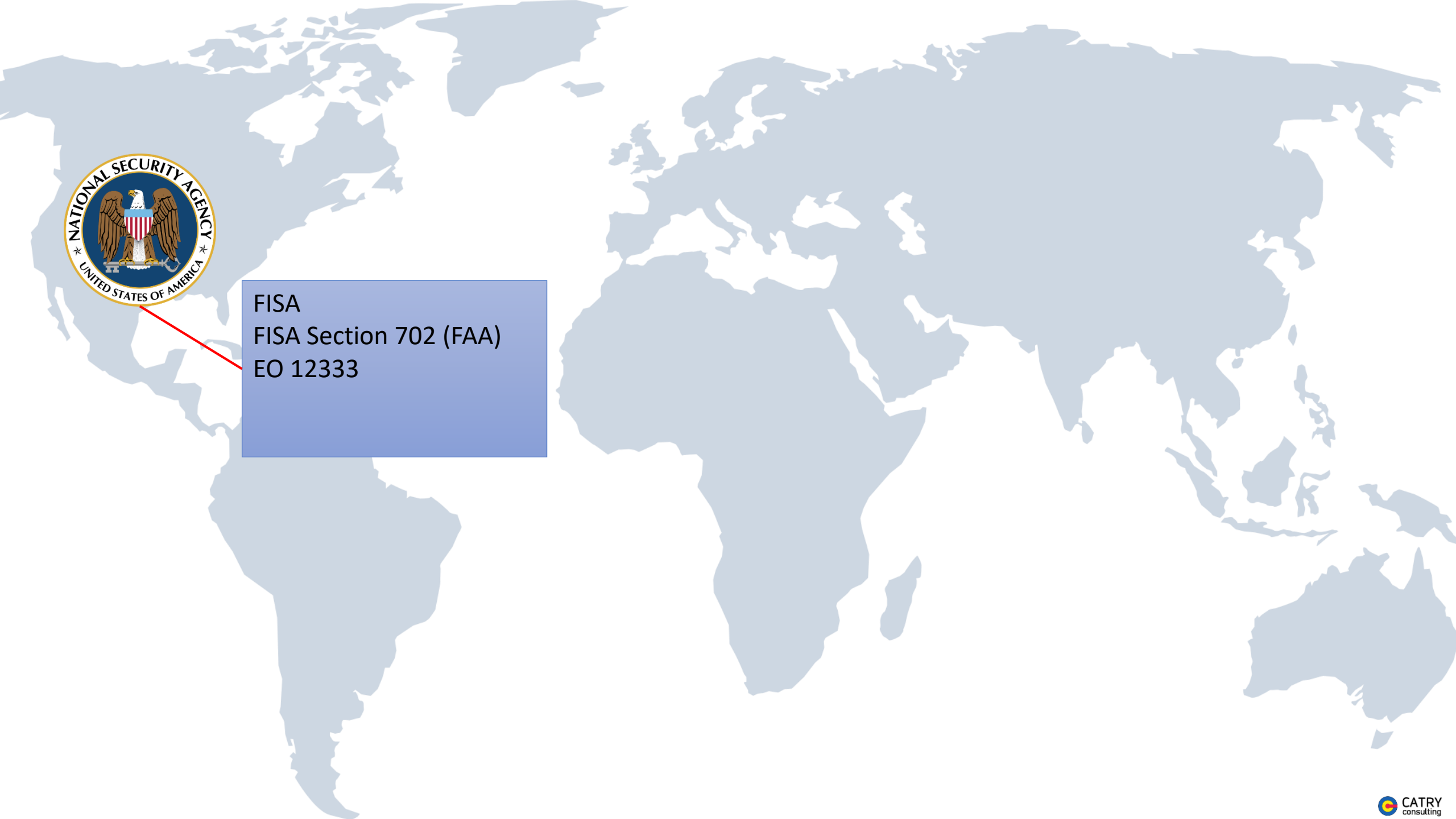
CATRY consulting

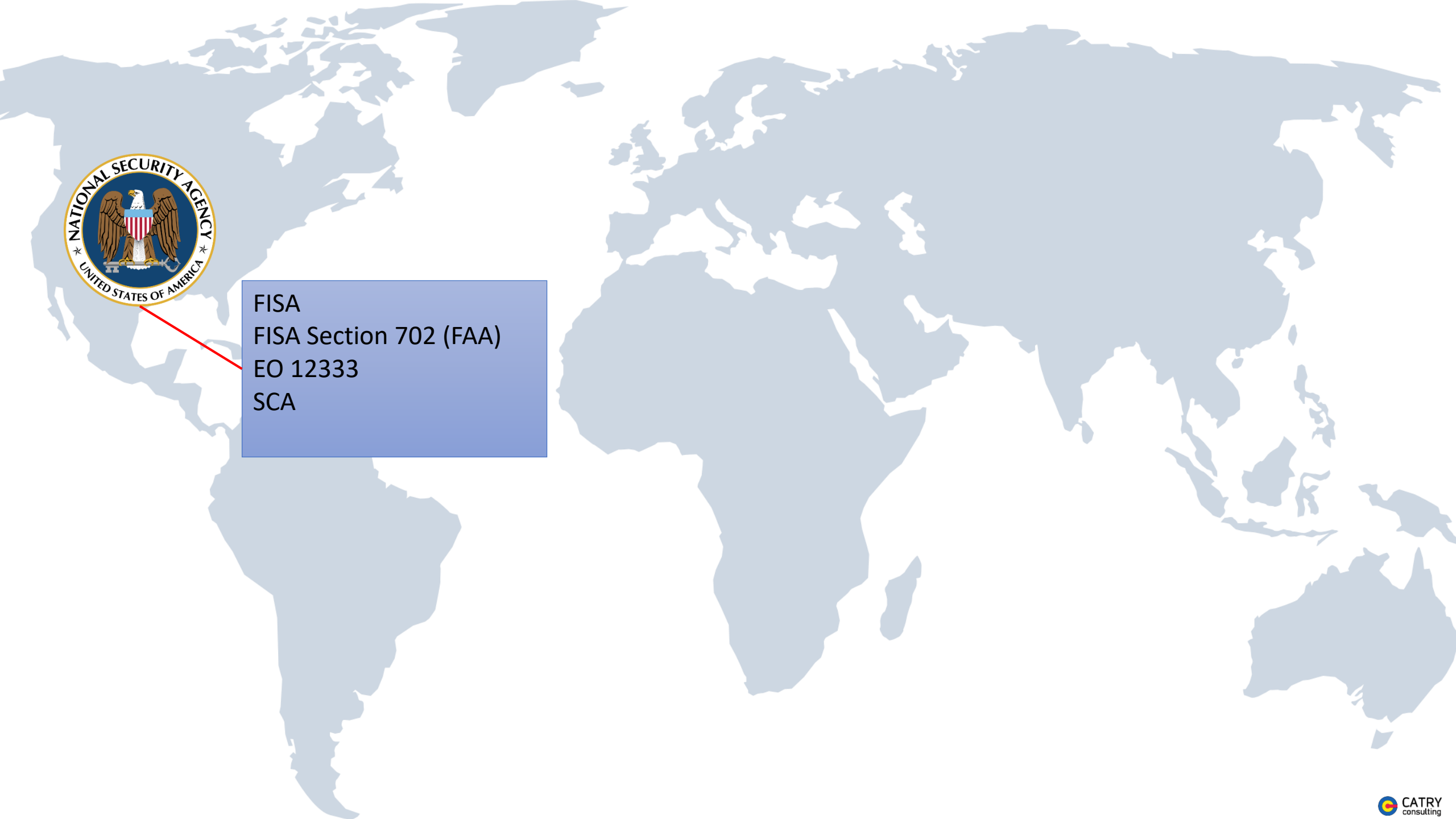
Inte bara USA

De flesta nationer har underrättelselagstiftning

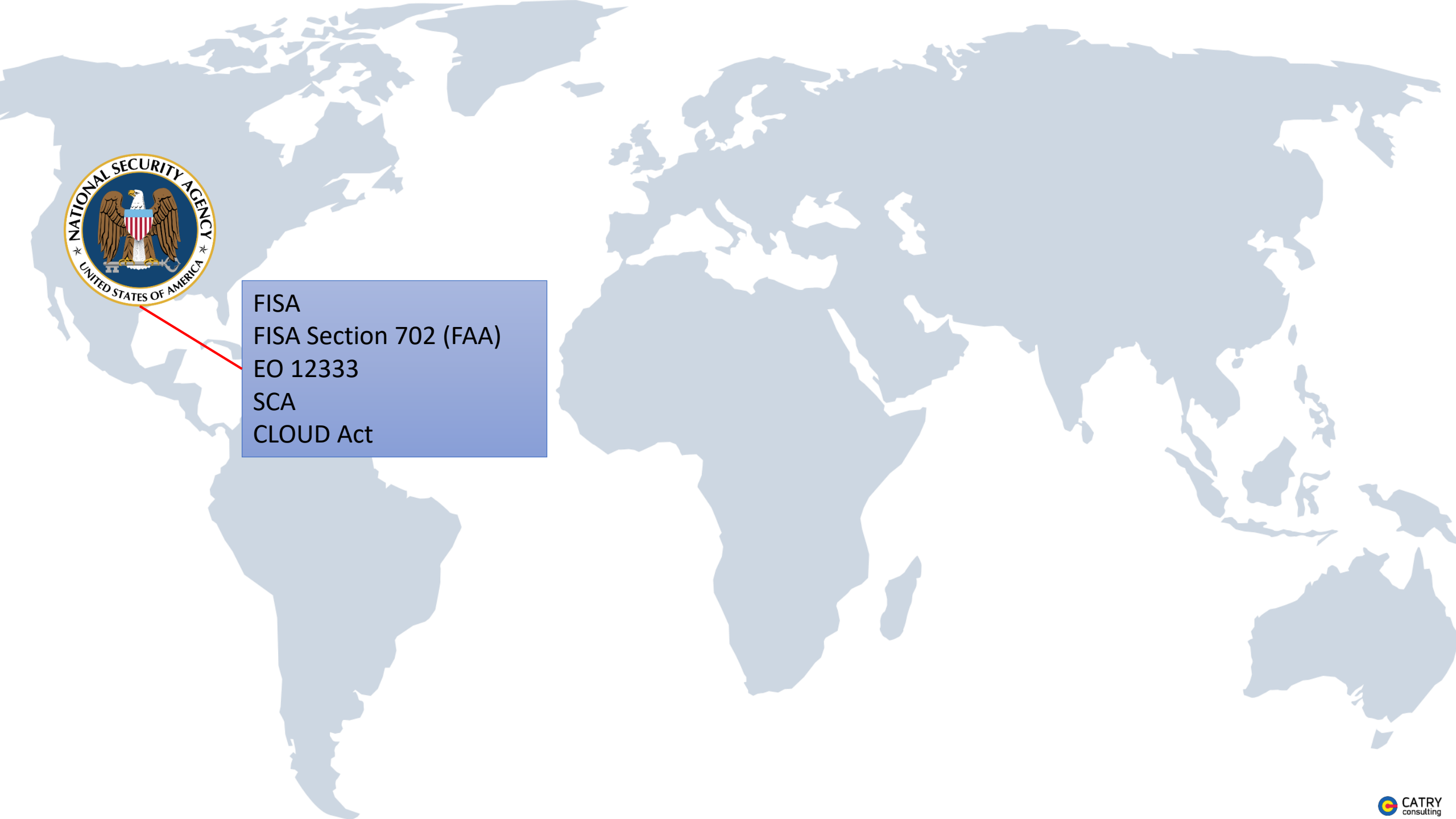




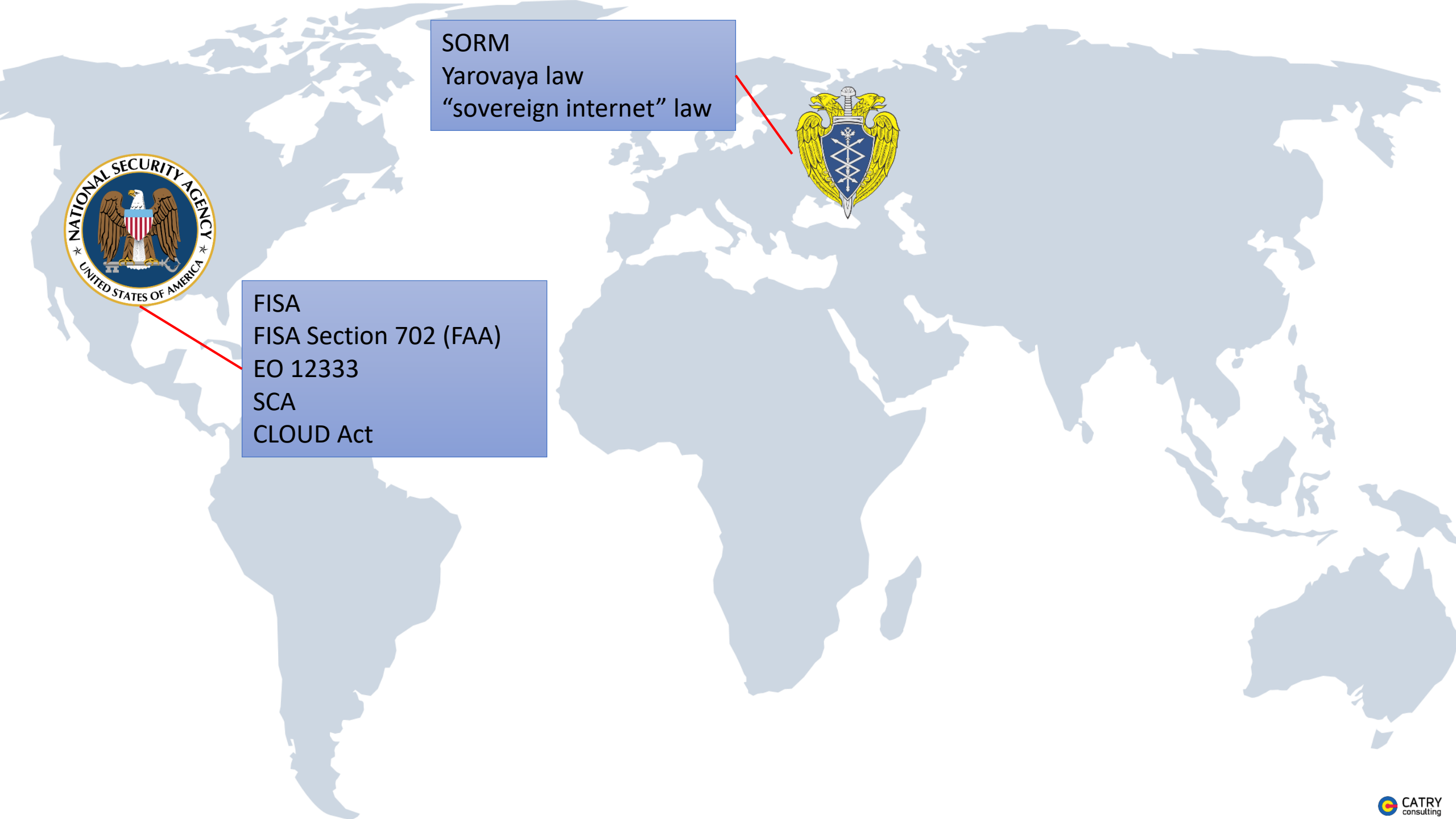




CATRY consulting



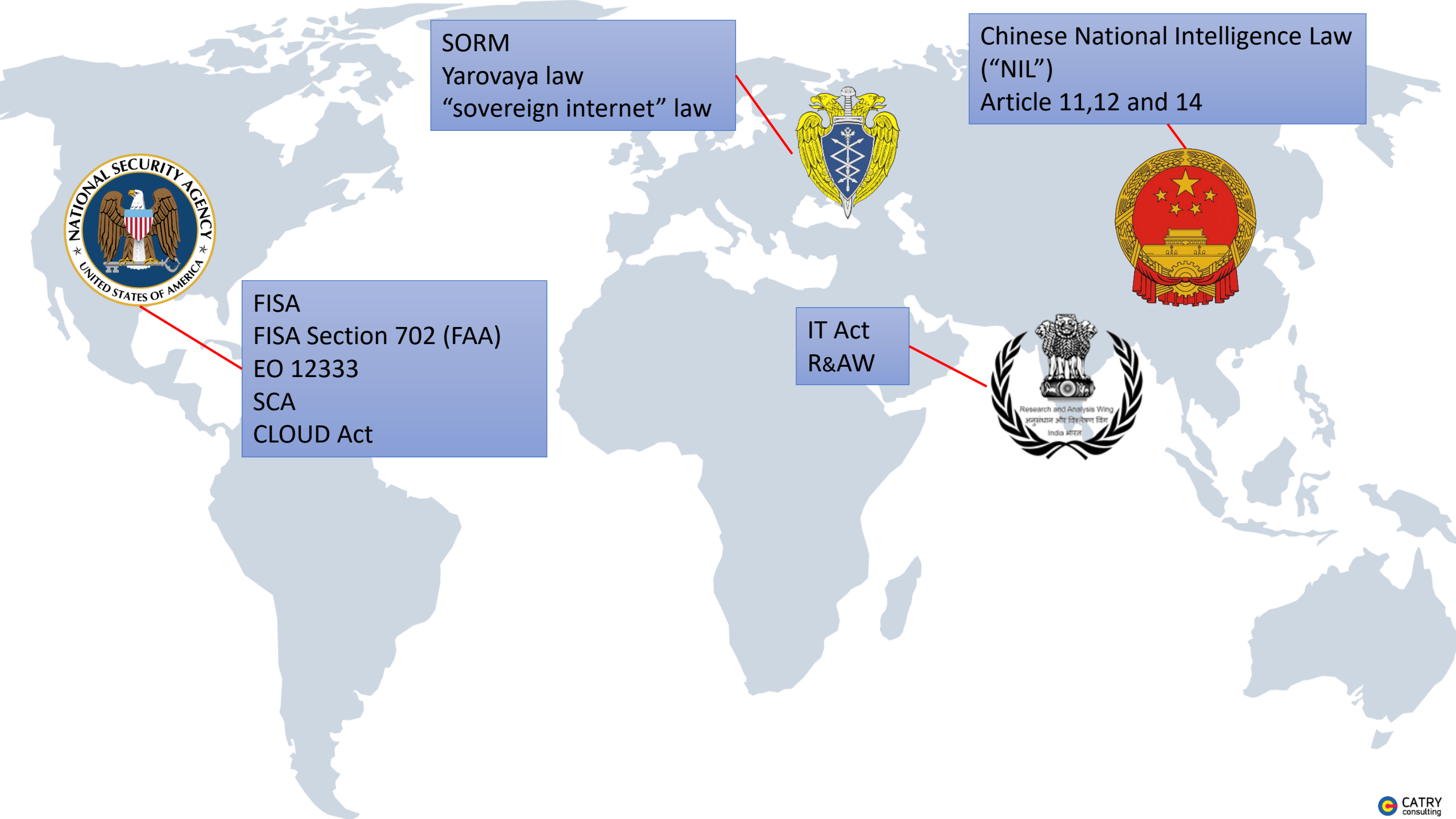
CATRY consulting



SORM
Yarovaya law
“sovereign internet” law

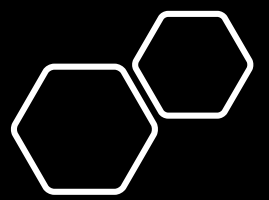
Chinese National Intelligence Law (“NIL”)
Article 11,12 and 14

FISA
FISA Section 702 (FAA)
EO 12333
SCA
CLOUD Act


SORM
Yarovaya law
“sovereign internet” law
Chinese National Intelligence Law
(“NIL”)
Article 11,12 and 14
FISA
FISA Section 702 (FAA)
EO 12333
SCA
CLOUD Act
IT Act
R&AW
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
Research and Analysis Wing
India

$$a_{i,j}^{(3)} = k_{i,j}^{(2)} + \sum_{\substack{e_2 \in \mathcal{E} \\ d_2 \in \mathcal{D}}} \frac{w_{i,e_2,d_2}}{\left(k_{e_2,e_2+j}^{(1)} + \sum_{\substack{e_1 \in \mathcal{E} \\ d_1 \in \mathcal{D}}} \frac{w_{e_2,e_1,d_1}}{\left(a_{e_1,e_1+e_2+j}^{(1)}\right)^{2^{d_1}}} \right)^{2^{d_2}}}$$

Kryptering
Advanced Encryption Standard (AES)



Kryptering

Data at rest

Encrypt inactive data when stored in blob storage, database, etc.

Data i vila

Data in transit

Encrypt data that is flowing between untrusted public or private networks

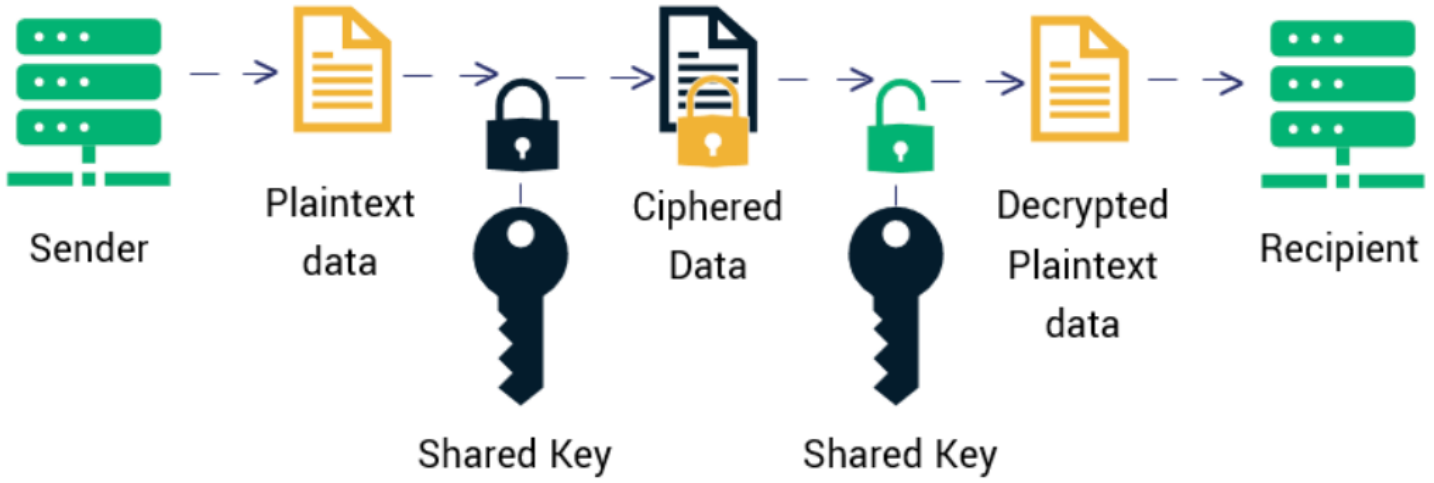
Transport

Data in use

Protect/encrypt data that is in use, while in RAM, and during computation

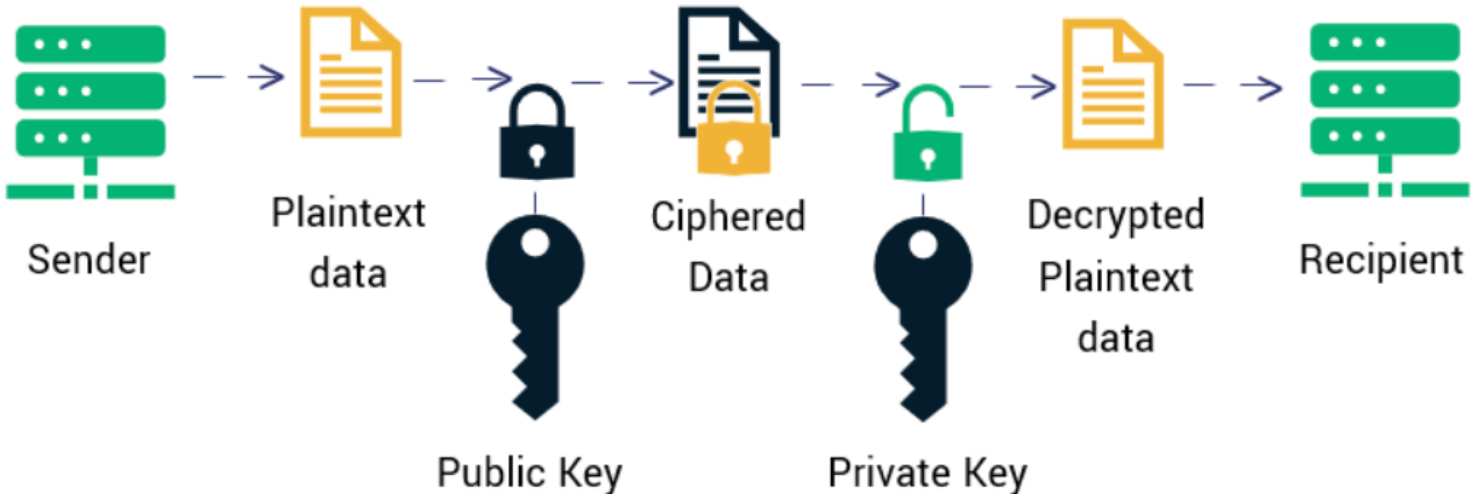
Används

Symmetrisk kryptering (samma nyckel)



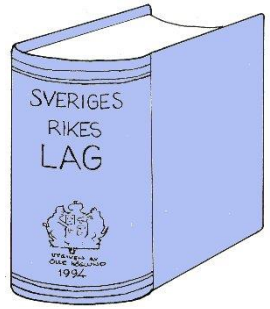
- Går att matematiskt bevisa
- Kan bara forceras med totalpröving s.k. brute-force-attacker
- Styrkan är beroende av nyckeln

Asymmetrisk kryptering (olika nycklar)



- Bygger på att något är svårt (exempelvis primtalsfaktorisering)
- Kan gå att hitta matematisk genvägar
- Sårbar mot kvantangrepp

Krypteringskrav i lagar?



KRYPTERING *OMNÄMNS* I VISSA FÖRFATTNINGAR!

- ***NIS 2 (artikel 21 h):*** Ett av säkerhetskraven (strategier och förfaranden för användning av kryptografi och, när så är lämpligt, *kryptering*)
- ***CSA (skäl 40):*** Exempel på områden där Enisa kan ge råd (främja grundläggande rådgivning om flerfaktorautentisering, programkorrigeringar, *kryptering*, anonymisering och dataskydd)
- ***SskL (4 kap. 4 §):*** Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras och skyddas med hjälp av *kryptografiska funktioner*, ska dessa ha godkänts av Försvarsmakten. Behörighet för FM att utfärda föreskrifter härom finns i Sskl 9 kap. 2 §
- ***SOU 2015:25 (s. 450):*** Hänvisar för närmare utformning av krypto till nationellt organ som utpekats att svara för detta, d.v.s. FM (s. 452)

MEN – KRYPTERING *DEFINIERAS INTE* I NÅGON FÖRFATTNING!

Kryptering – FM:s definitioner

FÖRSVARSMAKTEN (FM) GER VISSA DEFINITIONER (FFS 2021:1, 1 kap. 3 §)

- ***Kryptoalgoritm:*** *Matematiska funktioner i ett signalskyddssystem* för skydd av information mot röjande och förvanskning, identifiering och autentisering.
- ***Signalskyddsgrad:*** En indelning av ett signalskyddssystems *kryptologiska styrka* och vad signalskyddssystemet är godkänt för
- ***Signalskyddsmateriel:***
  1. *Kryptoapparat*, komponent, utrustning eller programvara som innehåller, eller avses innehålla, *kryptoalgoritmer* och som ingår, eller avses ingå, i ett signalskyddssystem.
  2. Annan signalskyddsspecifik materiel eller programvara.
- ***Signalskyddssystem:*** Av Försvarsmaktens högkvarter *godkänt system som innehåller kryptoalgoritm* för skydd av säkerhetskänslig verksamhet, inklusive säkerhetsskyddsklassificerade uppgifter, eller för trafikskydd.

”KRYPTERING” = Matematiska funktioner i ett signalskyddssystem…

Kryptering och legalitetsprincipen?

MEN – FM MEDDELAR JU SINA FÖRESKRIFTER MED STÖD I REGLERNA I SÄKERHETSSKYDDSLAGEN (SskL) OCH DE GÄLLER JU INTE GENERELLT I ALL SLAGS VERKSAMHET

- ***Så vad gäller då för annan verksamhet än sådan som omfattas av SskL?***
- ***Kan EDPB:s rekommendationer anses utgöra en generell rättskälla, eller gäller den bara när GDPR är tillämplig?***

- ***Kan FM:s eller EDPB:s alster tillämpas analogt?***
- ***EDPB:s riktlinjer/rekommendationer är inte rättsligt bindande, utan utgör endast råd och anvisningar…***
- ***Vilket värde och tyngd har dessa i så fall?***

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Version 2.0

Adopted on 18 June 2021

EDPB vägledning med avseende på kryptering

EDPB vägledning med avseende på kryptering

I de 7 användningsfall som beskriv i dokumentet går det att utläsa vad EDPB anser är kryptering.

Att just stark kryptering skall användas framgår av Användningsfall 1 punkt 1 ”personuppgifterna behandlas med användning av ***stark kryptering***”

Då ***starkt kryptering*** används ”anser EDPB att den kryptering som utförts utgör en effektiv kompletterande åtgärd”

EDPB vägledning med avseende på kryptering

I de 7 användningsfall som beskriv i dokumentet går det att utläsa vad EDPB anser är kryptering.

Att just stark kryptering skall användas framgår av Användningsfall 1 punkt 1 ”personuppgifterna behandlas med användning av ***stark kryptering***”

Då ***starkt kryptering*** används ”anser EDPB att den kryptering som utförts utgör en effektiv kompletterande åtgärd”

EDPB vägledning med avseende på kryptering

I de 7 användningsfall som beskriv i dokumentet går det att utläsa vad EDPB anser är kryptering.

Att just stark kryptering skall användas framgår av Användningsfall 1 punkt 1 ”personuppgifterna behandlas med användning av ***stark kryptering***”

Då ***starkt kryptering*** används ”anser EDPB att den kryptering som utförts utgör en effektiv kompletterande åtgärd”

Vad anser EDPB vara stark kryptering

Vad anser EDPB vara stark kryptering

- **Stark kryptering**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**
    - **Skall motstå totalprövning s.k. brute-force-attacker**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**
    - **Skall motstå totalprövning s.k. brute-force-attacker**
    - **Skall motstå både aktiva och passiva attacker**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**
    - **Skall motstå totalprövning s.k. brute-force-attacker**
    - **Skall motstå både aktiva och passiva attacker**
    - **Skyddar under den specifika tidsperiod för vilken personuppgifternas konfidentialitet måste upprätthållas**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**
    - **Skall motstå totalprövning s.k. brute-force-attacker**
    - **Skall motstå både aktiva och passiva attacker**
    - **Skyddar under den specifika tidsperiod för vilken personuppgifternas konfidentialitet måste upprätthållas**
  - **Förutsätter:**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**
    - **Skall motstå totalprövning s.k. brute-force-attacker**
    - **Skall motstå både aktiva och passiva attacker**
    - **Skyddar under den specifika tidsperiod för vilken personuppgifternas konfidentialitet måste upprätthållas**
  - **Förutsätter:**
    - **Krypteringsalgoritm skall vara robusta/motståndskraftiga mot kryptoanalys**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**
    - **Skall motstå totalprövning s.k. brute-force-attacker**
    - **Skall motstå både aktiva och passiva attacker**
    - **Skyddar under den specifika tidsperiod för vilken personuppgifternas konfidentialitet måste upprätthållas**
  - **Förutsätter:**
    - **Krypteringsalgoritm skall vara robusta/motståndskraftiga mot kryptoanalys**
    - **Parameterisering skall väljas för att försvåra kryptoanalys**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**
    - **Skall motstå totalprövning s.k. brute-force-attacker**
    - **Skall motstå både aktiva och passiva attacker**
    - **Skyddar under den specifika tidsperiod för vilken personuppgifternas konfidentialitet måste upprätthållas**
  - **Förutsätter:**
    - **Krypteringsalgoritm skall vara robusta/motståndskraftiga mot kryptoanalys**
    - **Parameterisering skall väljas för att försvåra kryptoanalys**
      - **Exempelvis så rekommenderas att när AES användas så skall någon av metoderna CBC, CFB, OFB eller CTR väljas med ej ECB.**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**
    - **Skall motstå totalprövning s.k. brute-force-attacker**
    - **Skall motstå både aktiva och passiva attacker**
    - **Skyddar under den specifika tidsperiod för vilken personuppgifternas konfidentialitet måste upprätthållas**
  - **Förutsätter:**
    - **Krypteringsalgoritm skall vara robusta/motståndskraftiga mot kryptoanalys**
    - **Parameterisering skall väljas för att försvåra kryptoanalys**
      - **Exempelvis så rekommenderas att när AES användas så skall någon av metoderna CBC, CFB, OFB eller CTR väljas med ej ECB.**
    - **Val av nyckellängd skall motstå en totalprövning (brute-force attack) av NSA**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**
    - **Skall motstå totalprövning s.k. brute-force-attacker**
    - **Skall motstå både aktiva och passiva attacker**
    - **Skyddar under den specifika tidsperiod för vilken personuppgifternas konfidentialitet måste upprätthållas**
  - **Förutsätter:**
    - **Krypteringsalgoritm skall vara robusta/motståndskraftiga mot kryptoanalys**
    - **Parameterisering skall väljas för att försvåra kryptoanalys**
      - **Exempelvis så rekommenderas att när AES användas så skall någon av metoderna CBC, CFB, OFB eller CTR väljas med ej ECB.**
    - **Val av nyckellängd skall motstå en totalprövning (brute-force attack) av NSA**
    - **Korrekt implementering – kan verifieras genom certifiering**

Vad anser EDPB vara stark kryptering

- **Stark kryptering**
  - **Krav:**
    - **Skall skydda under transport, förvar och process**
    - **Skall motstå kryptoanalys**
    - **Skall motstå totalprövning s.k. brute-force-attacker**
    - **Skall motstå både aktiva och passiva attacker**
    - **Skyddar under den specifika tidsperiod för vilken personuppgifternas konfidentialitet måste upprätthållas**
  - **Förutsätter:**
    - **Krypteringsalgoritm skall vara robusta/motståndskraftiga mot kryptoanalys**
    - **Parameterisering skall väljas för att försvåra kryptoanalys**
      - **Exempelvis så rekommenderas att när AES användas så skall någon av metoderna CBC, CFB, OFB eller CTR väljas med ej ECB.**
    - **Val av nyckellängd skall motstå en totalprövning (brute-force attack) av NSA**
    - **Korrekt implementering – kan verifieras genom certifiering**
    - **Säker nyckelhantering vid generering, administration, lagring**

Vad anser EDPB vara stark kryptering

Vad anser EDPB vara stark kryptering

1. Uppgifterna ska skyddas genom tillämpning av stark kryptering innan överföring sker;

Vad anser EDPB vara stark kryptering

1. Uppgifterna ska skyddas genom tillämpning av stark kryptering innan överföring sker;

2. Krypteringsmetoderna som används skall motstå kryptoanalys utförd med sådana resurser som utländska myndigheter kan tänkas förfoga över;

Vad anser EDPB vara stark kryptering

1. Uppgifterna ska skyddas genom tillämpning av stark kryptering innan överföring sker;
2. Krypteringsmetoderna som används skall motstå kryptoanalys utförd med sådana resurser som utländska myndigheter kan tänkas förfoga över;
3. Krypteringsmetoderna skall motstå den tekniska utveckling som kan tänkas ske under den tid uppgifterna behandlas, inklusive så kallad totalprövning (eng. ”brute-force”);

Vad anser EDPB vara stark kryptering

1. Uppgifterna ska skyddas genom tillämpning av stark kryptering innan överföring sker;
2. Krypteringsmetoderna som används skall motstå kryptoanalys utförd med sådana resurser som utländska myndigheter kan tänkas förfoga över;
3. Krypteringsmetoderna skall motstå den tekniska utveckling som kan tänkas ske under den tid uppgifterna behandlas, inklusive så kallad totalprövning (eng. ”brute-force”);
4. Krypteringsalgoritmerna ska vara korrekt införda i systemen, och det ska verifieras (t.ex. genom certifiering) att funktionerna är fria från sårbarheter;

Vad anser EDPB vara stark kryptering

1. Uppgifterna ska skyddas genom tillämpning av stark kryptering innan överföring sker;
2. Krypteringsmetoderna som används skall motstå kryptoanalys utförd med sådana resurser som utländska myndigheter kan tänkas förfoga över;
3. Krypteringsmetoderna skall motstå den tekniska utveckling som kan tänkas ske under den tid uppgifterna behandlas, inklusive så kallad totalprövning (eng. ”brute-force”);
4. Krypteringsalgoritmerna ska vara korrekt införda i systemen, och det ska verifieras (t.ex. genom certifiering) att funktionerna är fria från sårbarheter;
5. Krypteringsnycklar ska skapas, lagras, användas och förstöras på ett säkert sätt;

Vad anser EDPB vara stark kryptering

1. Uppgifterna ska skyddas genom tillämpning av stark kryptering innan överföring sker;

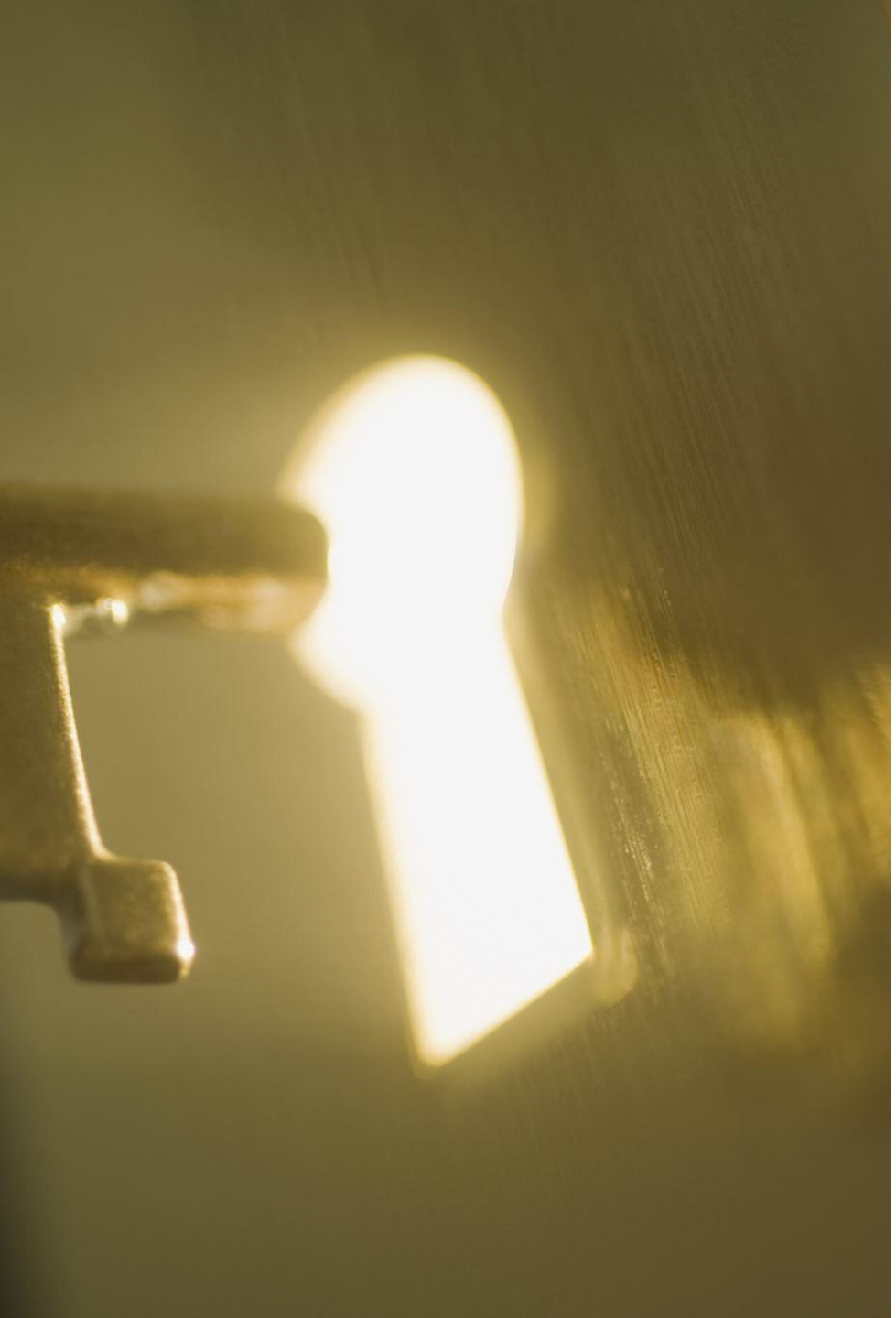
2. Krypteringsmetoderna som används skall motstå kryptoanalys utförd med sådana resurser som utländska myndigheter kan tänkas förfoga över;

3. Krypteringsmetoderna skall motstå den tekniska utveckling som kan tänkas ske under den tid uppgifterna behandlas, inklusive så kallad totalprövning (eng. ”brute-force”);

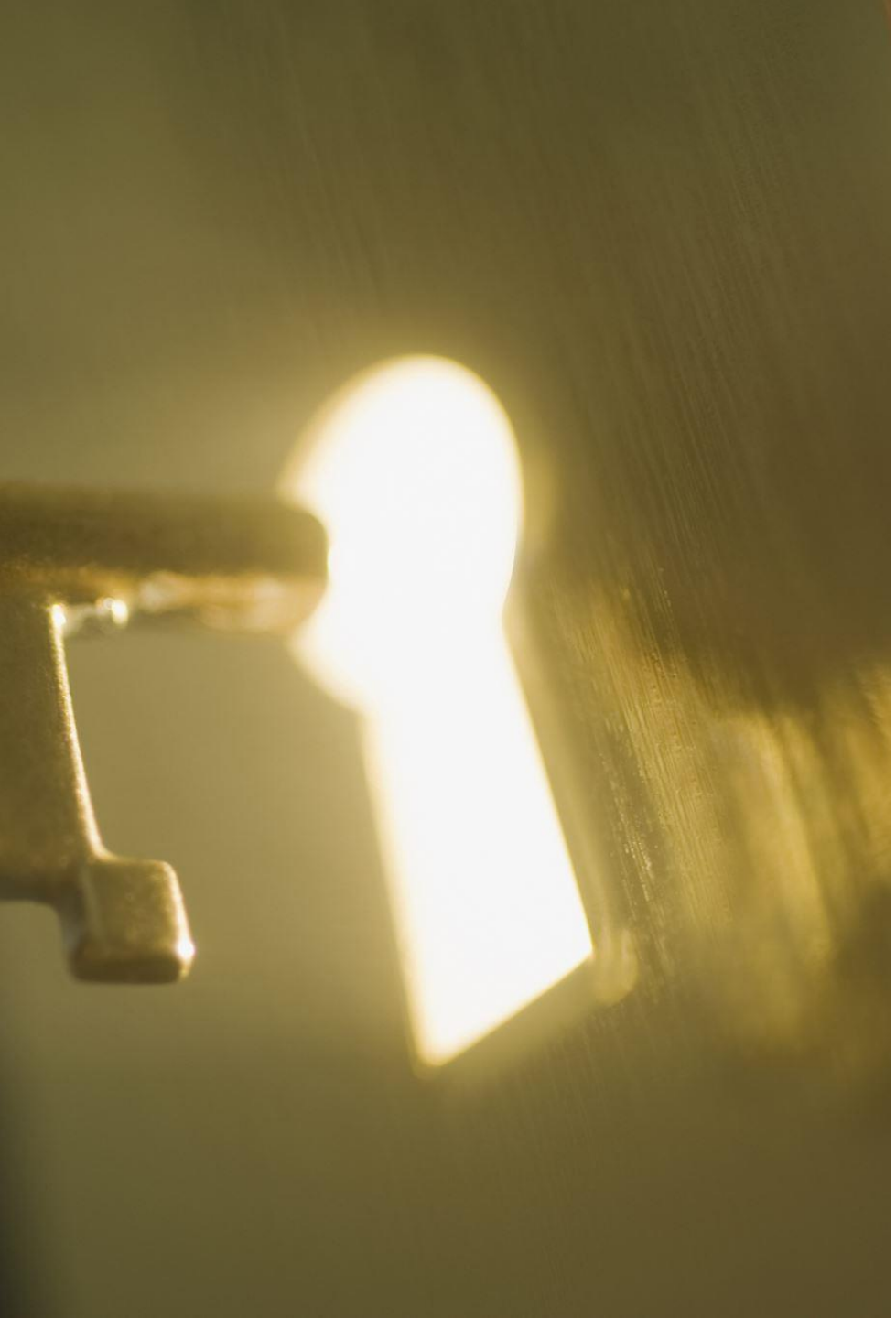
4. Krypteringsalgoritmerna ska vara korrekt införda i systemen, och det ska verifieras (t.ex. genom certifiering) att funktionerna är fria från sårbarheter;

5. Krypteringsnycklar ska skapas, lagras, användas och förstöras på ett säkert sätt;

6. Krypteringsnycklarna ska helt och hållet förvaras så att de endast kan brukas av personuppgiftsansvarig (eller av denne utsett personuppgiftsbiträde som är verksam inom EU/EES eller inom en jurisdiktion med adekvat skyddsnivå), dvs, nyckelmaterialet hålls fullständigt oåtkomligt för leverantören för såväl åtkomst som användning.

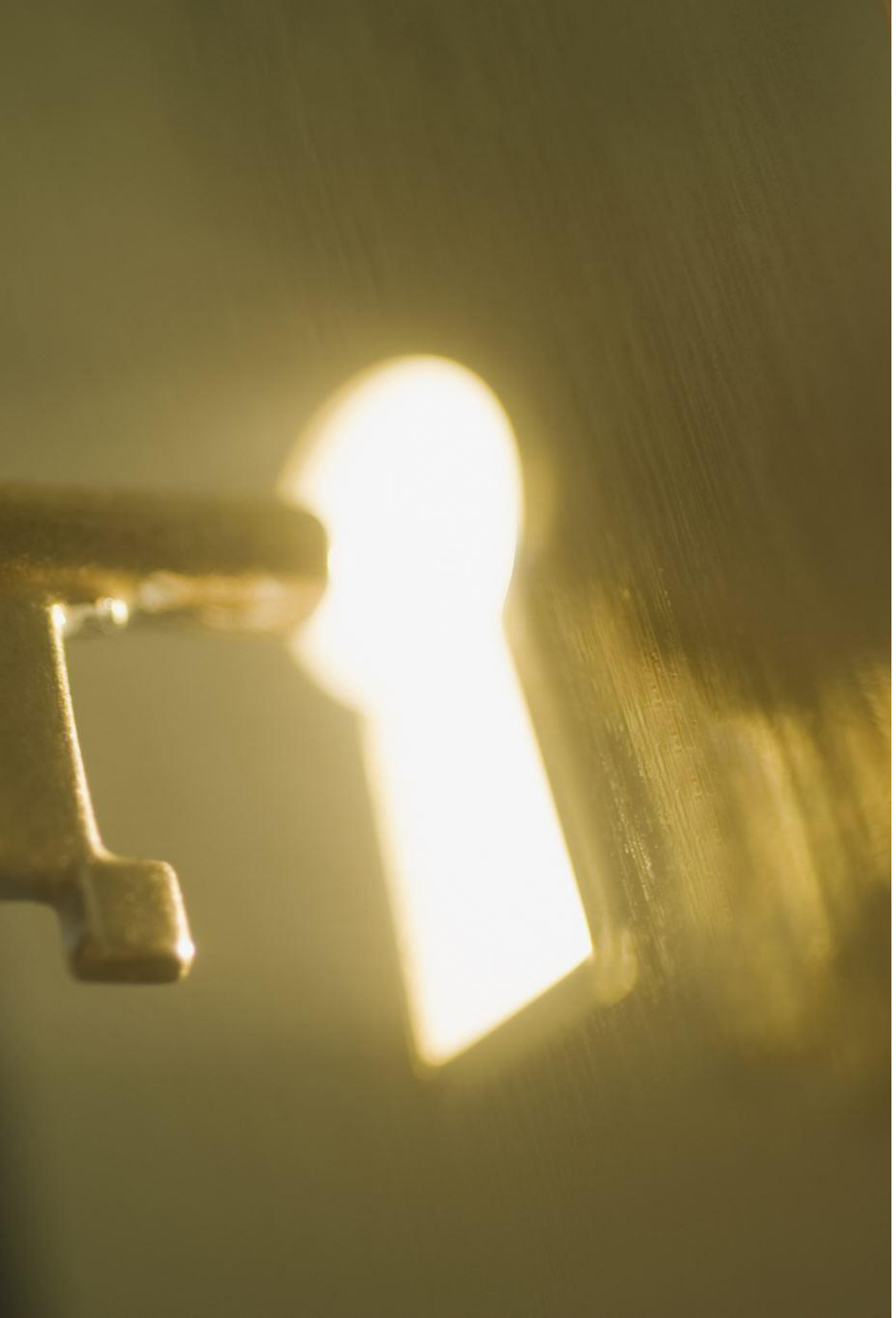


Krypteringsnyckeln är nyckeln



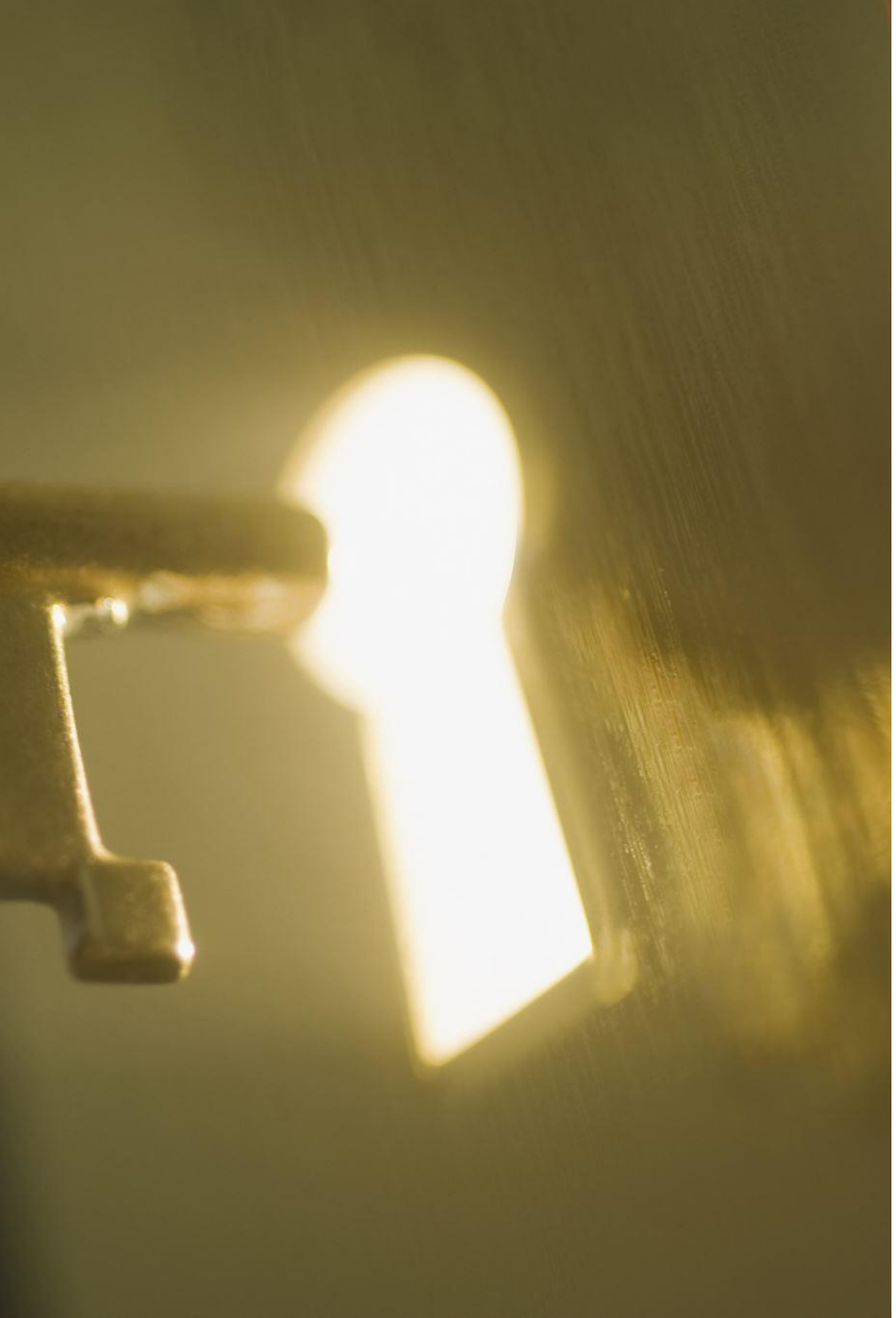
Krypteringsnyckeln är nyckeln

- Leverantören garanterar att det inte kan lämna ut kundens krypteringsnyckel ”***Vi ger inte någon myndighet tillgång till våra krypteringsnycklar eller möjlighet att bryta vår kryptering”***



Krypteringsnyckeln är nyckeln

- Leverantören garanterar att det inte kan lämna ut kundens krypteringsnyckel ”***Vi ger inte någon myndighet tillgång till våra krypteringsnycklar eller möjlighet att bryta vår kryptering”***
- Punkt 81 ”As an example, U.S. data importers that fall under 50 USC § 1881a (FISA 702) are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible.”



Krypteringsnyckeln är nyckeln

- Leverantören garanterar att det inte kan lämna ut kundens krypteringsnyckel ”***Vi ger inte någon myndighet tillgång till våra krypteringsnycklar eller möjlighet att bryta vår kryptering”***
- Punkt 81 ”As an example, U.S. data importers that fall under 50 USC § 1881a (FISA 702) are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible.”
- Okej - men ***vi har gjort det teknisk omöjligt för oss att lämna ut kundens nyckel***.

Tjänstkryptering SharePoint Online

- Nycklarna som används för att kryptera blobarna lagras i SharePoint Online-innehållsdatabasen. SharePoint Online-innehållsdatabasen skyddas av databasåtkomstkontroller och kryptering i vila. Kryptering utförs med hjälp av TDE i Azure SQL Database. Dessa hemligheter finns på tjänstnivå för SharePoint Online, inte på klientorganisationsnivå. Dessa hemligheter (kallas ibland för huvudnycklar) lagras på en separat säker lagringsplats som kallas nyckellagringsplats. TDE ger säkerhet i vila för både den aktiva databasen och databassäkerhetskopiorna och transaktionsloggarna. När kunder tillhandahåller den valfria nyckeln lagras kundnyckeln i Azure Key Vault och tjänsten använder nyckeln för att kryptera en klientnyckel, som används för att kryptera en platsnyckel, som sedan används för att kryptera filnivånycklarna. I princip introduceras en ny nyckelhierarki när kunden tillhandahåller en nyckel.

https://learn.microsoft.com/sv-se/microsoft-365/compliance/office-365-encryption-risks-and-protections?view=o365-worldwide

Tjänstkryptering SharePoint Online

- Nycklarna som används för att kryptera blobarna lagras i SharePoint Online-innehållsdatabasen. SharePoint Online-innehållsdatabasen skyddas av databasåtkomstkontroller och kryptering i vila. Kryptering utförs med hjälp av TDE i Azure SQL Database. Dessa hemligheter finns på tjänstnivå för SharePoint Online, inte på klientorganisationsnivå. Dessa hemligheter (kallas ibland för huvudnycklar) lagras på en separat säker lagringsplats som kallas nyckellagringsplats. TDE ger säkerhet i vila för både den aktiva databasen och databassäkerhetskopiorna och transaktionsloggarna. När kunder tillhandahåller den valfria nyckeln lagras kundnyckeln i Azure Key Vault och tjänsten använder nyckeln för att kryptera en klientnyckel, som används för att kryptera en platsnyckel, som sedan används för att kryptera filnivånycklarna. I princip introduceras en ny nyckelhierarki när kunden tillhandahåller en nyckel.

https://learn.microsoft.com/sv-se/microsoft-365/compliance/office-365-encryption-risks-and-protections?view=o365-worldwide

Tjänstkryptering SharePoint Online

- Nycklarna som används för att kryptera blobarna lagras i SharePoint Online-innehållsdatabasen. SharePoint Online-innehållsdatabasen skyddas av databasåtkomstkontroller och kryptering i vila. Kryptering utförs med hjälp av TDE i Azure SQL Database. Dessa hemligheter finns på tjänstnivå för SharePoint Online, inte på klientorganisationsnivå. Dessa hemligheter (kallas ibland för huvudnycklar) lagras på en separat säker lagringsplats som kallas nyckellagringsplats. TDE ger säkerhet i vila för både den aktiva databasen och databassäkerhetskopiorna och transaktionsloggarna. När kunder tillhandahåller den valfria nyckeln lagras kundnyckeln i Azure Key Vault och tjänsten använder nyckeln för att kryptera en klientnyckel, som används för att kryptera en platsnyckel, som sedan används för att kryptera filnivånycklarna. I princip introduceras en ny nyckelhierarki när kunden tillhandahåller en nyckel.

https://learn.microsoft.com/sv-se/microsoft-365/compliance/office-365-encryption-risks-and-protections?view=o365-worldwide

Tjänstkryptering SharePoint Online

- Nycklarna som används för att kryptera blobarna lagras i SharePoint Online-innehållsdatabasen. SharePoint Online-innehållsdatabasen skyddas av databasåtkomstkontroller och kryptering i vila. Kryptering utförs med hjälp av TDE i Azure SQL Database. Dessa hemligheter finns på tjänstnivå för SharePoint Online, inte på klientorganisationsnivå. Dessa hemligheter (kallas ibland för huvudnycklar) lagras på en separat säker lagringsplats som kallas nyckellagringsplats. TDE ger säkerhet i vila för både den aktiva databasen och databassäkerhetskopiorna och transaktionsloggarna. När kunder tillhandahåller den valfria nyckeln lagras kundnyckeln i Azure Key Vault och tjänsten använder nyckeln för att kryptera en klientnyckel, som används för att kryptera en platsnyckel, som sedan används för att kryptera filnivånycklarna. I princip introduceras en ny nyckelhierarki när kunden tillhandahåller en nyckel.

https://learn.microsoft.com/sv-se/microsoft-365/compliance/office-365-encryption-risks-and-protections?view=o365-worldwide

Tjänstkryptering SharePoint Online

- Nycklarna som används för att kryptera blobarna lagras i SharePoint Online-innehållsdatabasen. SharePoint Online-innehållsdatabasen skyddas av databasåtkomstkontroller och kryptering i vila. Kryptering utförs med hjälp av TDE i Azure SQL Database. Dessa hemligheter finns på tjänstnivå för SharePoint Online, inte på klientorganisationsnivå. Dessa hemligheter (kallas ibland för huvudnycklar) lagras på en separat säker lagringsplats som kallas nyckellagringsplats. TDE ger säkerhet i vila för både den aktiva databasen och databassäkerhetskopiorna och transaktionsloggarna. När kunder tillhandahåller den valfria nyckeln lagras kundnyckeln i Azure Key Vault och tjänsten använder nyckeln för att kryptera en klientnyckel, som används för att kryptera en platsnyckel, som sedan används för att kryptera filnivånycklarna. I princip introduceras en ny nyckelhierarki när kunden tillhandahåller en nyckel.

https://learn.microsoft.com/sv-se/microsoft-365/compliance/office-365-encryption-risks-and-protections?view=o365-worldwide

Tjänstkryptering SharePoint Online

- Nycklarna som används för att kryptera blobarna lagras i SharePoint Online-innehållsdatabasen. SharePoint Online-innehållsdatabasen skyddas av databasåtkomstkontroller och kryptering i vila. Kryptering utförs med hjälp av TDE i Azure SQL Database. Dessa hemligheter finns på tjänstnivå för SharePoint Online, inte på klientorganisationsnivå. Dessa hemligheter (kallas ibland för huvudnycklar) lagras på en separat säker lagringsplats som kallas nyckellagringsplats. TDE ger säkerhet i vila för både den aktiva databasen och databassäkerhetskopiorna och transaktionsloggarna. När kunder tillhandahåller den valfria nyckeln lagras kundnyckeln i Azure Key Vault och tjänsten använder nyckeln för att kryptera en klientnyckel, som används för att kryptera en platsnyckel, som sedan används för att kryptera filnivånycklarna. I princip introduceras en ny nyckelhierarki när kunden tillhandahåller en nyckel.

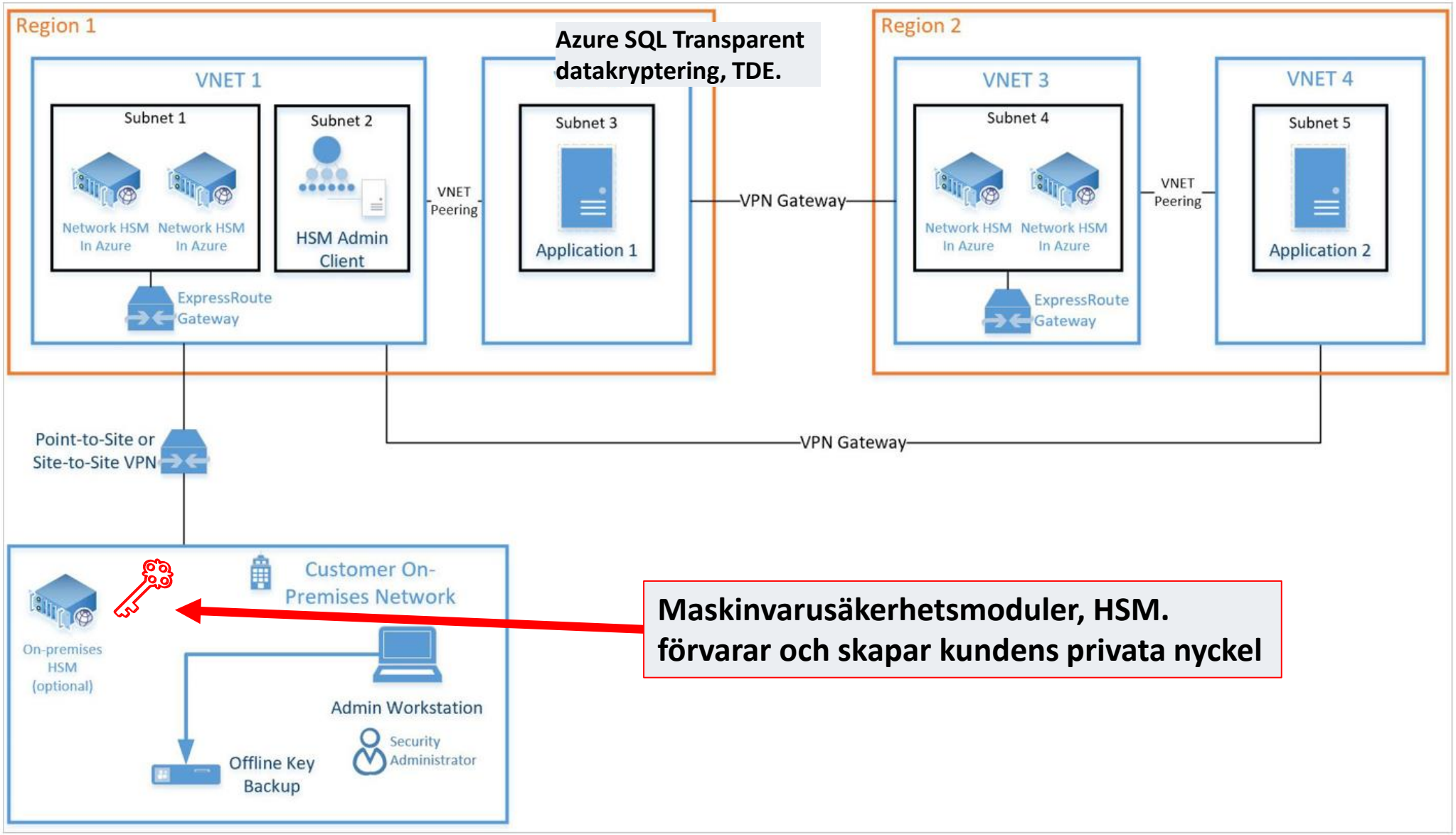
https://learn.microsoft.com/sv-se/microsoft-365/compliance/office-365-encryption-risks-and-protections?view=o365-worldwide

Tjänstkryptering SharePoint Online

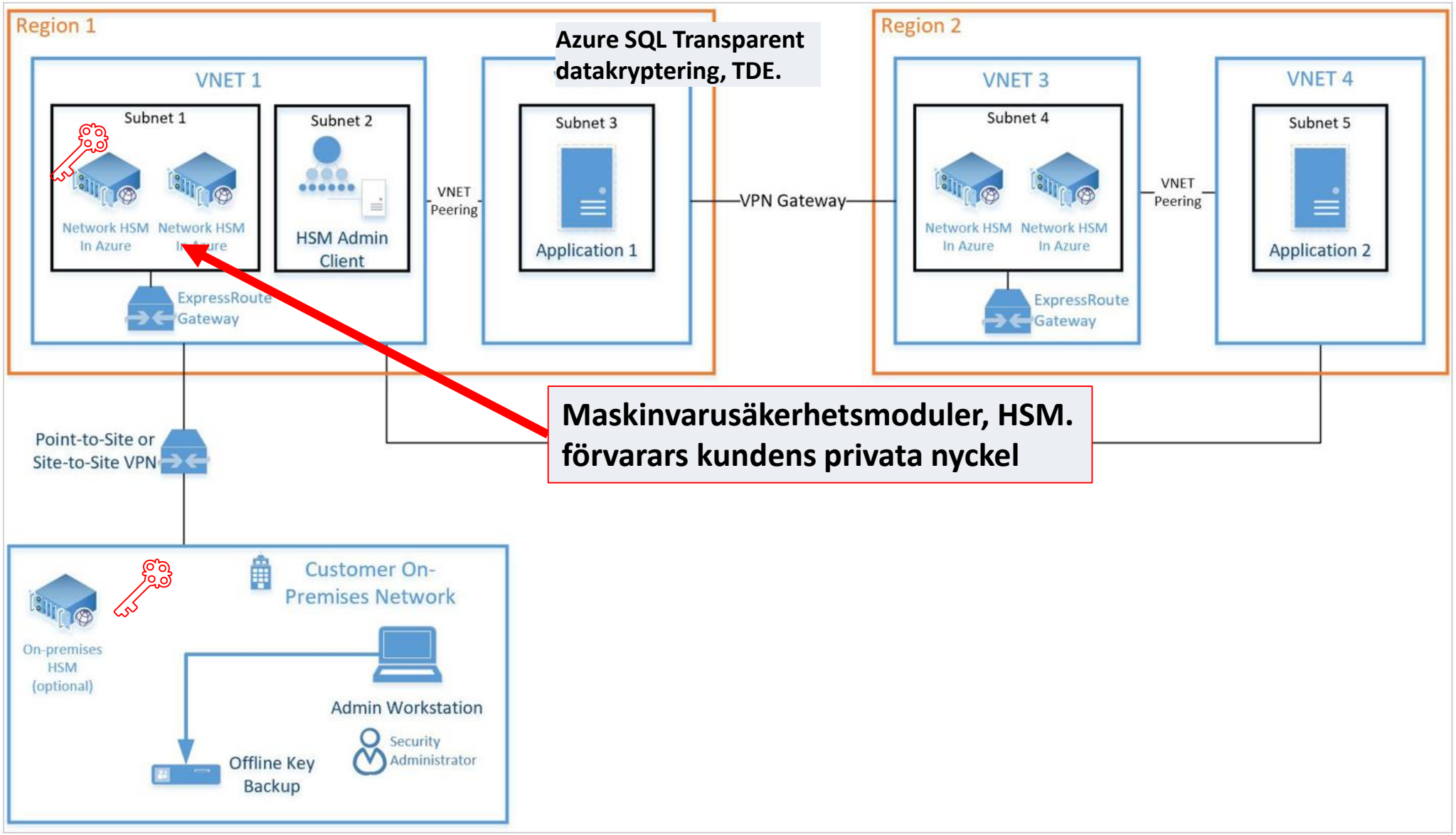
- Nycklarna som används för att kryptera blobarna lagras i SharePoint Online-innehållsdatabasen. SharePoint Online-innehållsdatabasen skyddas av databasåtkomstkontroller och kryptering i vila. Kryptering utförs med hjälp av TDE i Azure SQL Database. Dessa hemligheter finns på tjänstnivå för SharePoint Online, inte på klientorganisationsnivå. Dessa hemligheter (kallas ibland för huvudnycklar) lagras på en separat säker lagringsplats som kallas nyckellagringsplats. TDE ger säkerhet i vila för både den aktiva databasen och databassäkerhetskopiorna och transaktionsloggarna. När kunder tillhandahåller den valfria nyckeln lagras kundnyckeln i Azure Key Vault och tjänsten använder nyckeln för att kryptera en klientnyckel, som används för att kryptera en platsnyckel, som sedan används för att kryptera filnivånycklarna. I princip introduceras en ny nyckelhierarki när kunden tillhandahåller en nyckel.

https://learn.microsoft.com/sv-se/microsoft-365/compliance/office-365-encryption-risks-and-protections?view=o365-worldwide

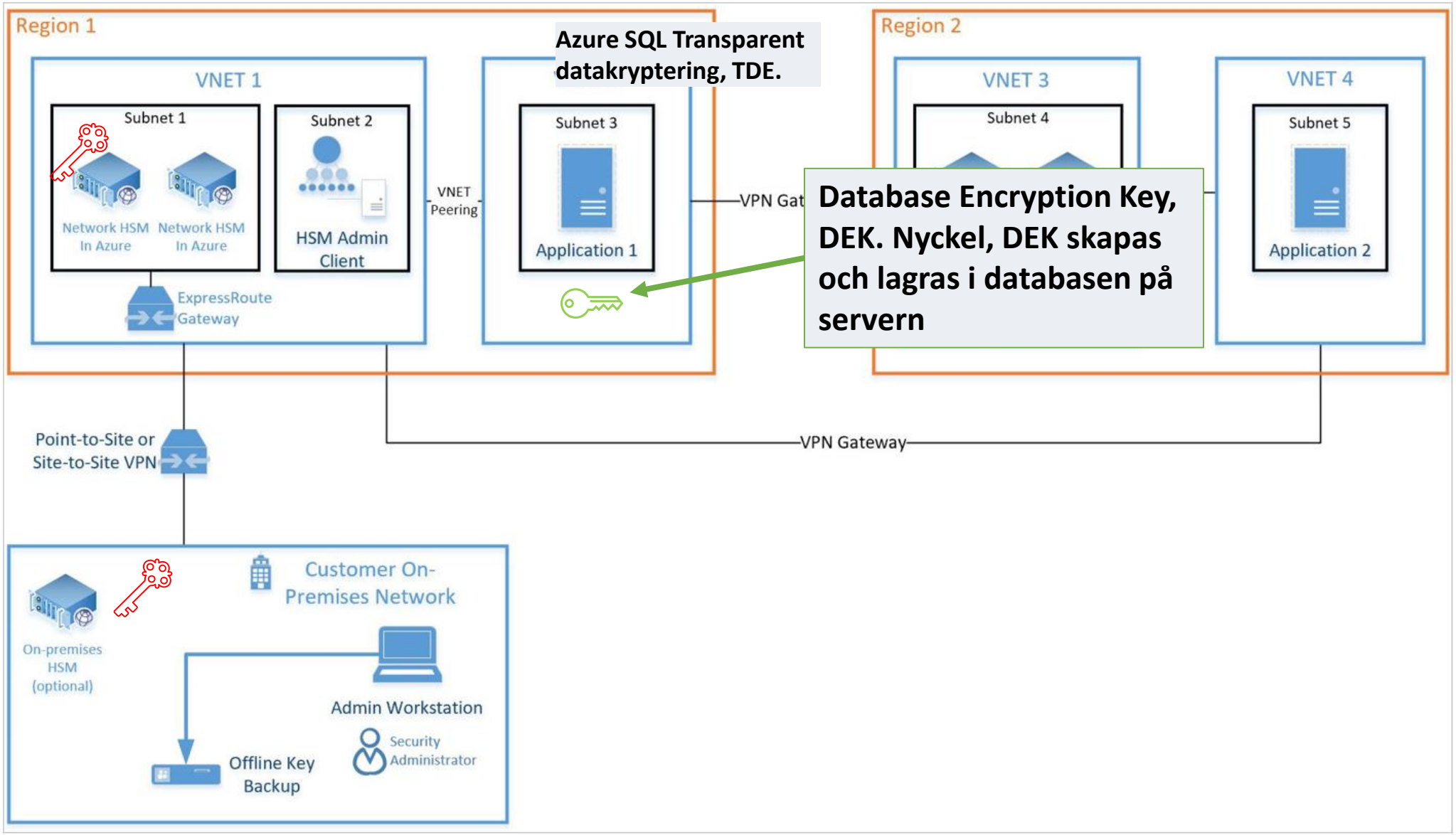
Bring Your Own Key (BYOK) lösning med HSM



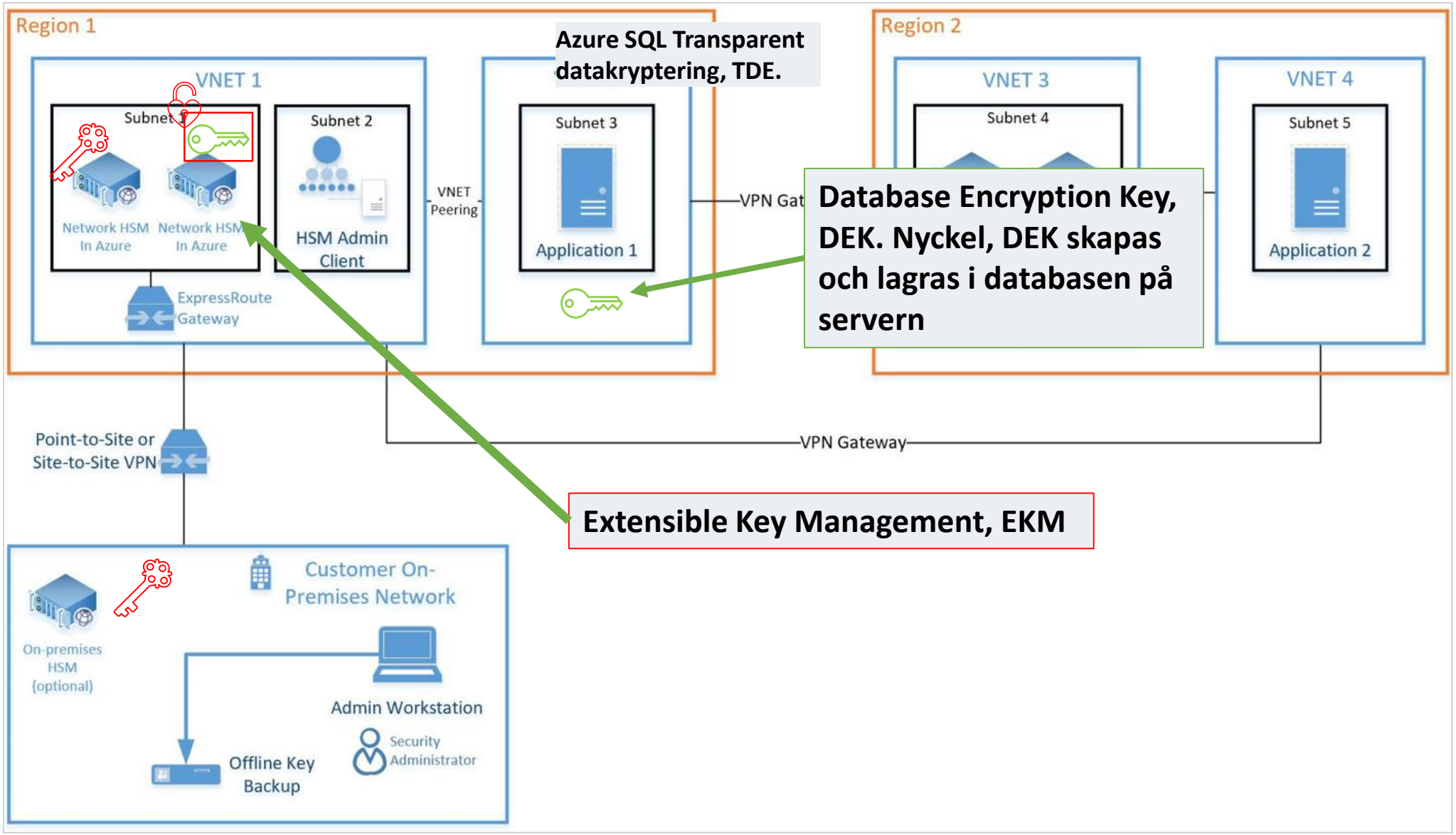
Bring Your Own Key (BYOK) lösning med HSM



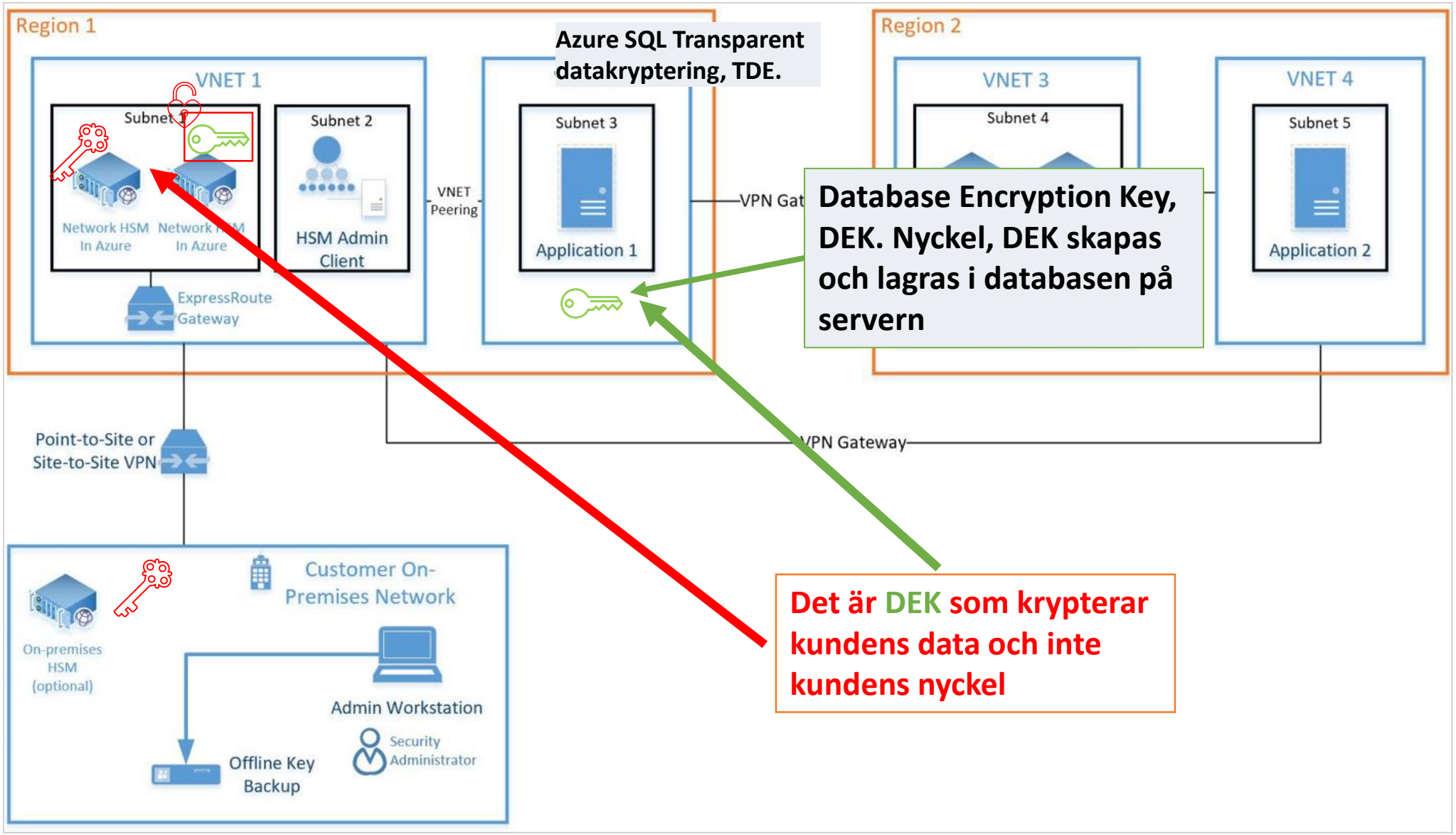
Bring Your Own Key (BYOK) lösning med HSM



Bring Your Own Key (BYOK) lösning med HSM



Bring Your Own Key (BYOK) lösning med HSM



C-Resiliens AB

André Catry

andre@catry.se

0761-81 12 13