LAVORO DI GRUPPO n.1 – ANALISI E VALUTAZIONE DELLE POLITICHE PUBBLICHE (UNIMI) – a.a. 2020/2021

NATIONAL CYBER SECURITY STRATEGY 2016-2021

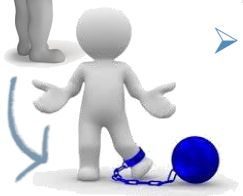
ASSERO – BARAZZETTA – BIANCHI - BISSANTI – CAVANNA – COLOMBO – MIDURI - SALA

NATIONAL CYBER SECURITY STRATEGY '16-'21

IL PERCORSO: L'ANALISI DEL REPORT E LA METAVALUTAZIONE

1. LE CARATTERISTICHE DEL NAO

Il *National Audit Office* è il principale «whatchdog» nella valutazionbe delle politiche in Britanniche.
LE INDAGINI IN CHIAVE VALUTATIVA RIGUARDANO SPECIALMENTE 5 AREE DI LAVORO



2. L'ORIGINE DELLA POLICY

Tra i report disponibili nel sito abbiamo individuato **LA VALUTAZIONE EFFETTUATA RISPETTO AL CYBER SECURITY STRATEGY 2016-2021,** nata con l'esigenza di individuare una strategia efficace per contrastare gli attacchi informatici

3. STRUMENTI, FINANZIAMENTI, STRUTTURA

Per favorire l'implementazione di azioni finalizzate alla sicurezza informatica sono stati utilizzati diversi **STRUMENTI NORMATIVI DI CARATTERE REGOLATORIO**, un budget notevole e una **STRUTTURA DECISIONALE MOLTO ARTICOLATA**

4. IMPLEMENTAZIONE: POLICY TOOLS, ATTORI, INIZIATIVE

Il governo, il National Cyber Security Centre(NCSC), National Cyber Force (NCF) sono **PROTAGONISTI NEL MONITORAGGIO E NELL'ATTUAZIONE** di politiche per la sicurezza informatica

5. CHE TIPO DI VALUTAZIONE?

Nella valutazione delle politiche già concluse in tema cyber security il report presenta un **ANALISI EX-POST**, mentre sulle fasi attuali nella strategia più recente emerge una **VALUTAZIONE IN ITINERE**

6. ANALISI DEL REPORT: I METODI DI RICERCA

Oltre ai metodi di ricerca ricorrenti emerge la presenza di **ANALISI AD HOC** di specifici fattori.

7. METAVALUTAZIONE

Il report presenta una chiara divisione del lavoro e presentazione dei risultati e delle criticità emerse;
la suddivisione in 4 parti genera una visione chiara del tema affrontato e delle sfaccettature date ad esso.
LA STRATEGIA VALUTATA SI RIVELA COMPLESSIVAMENTE ADEGUATA E IN ALCUNI ASPETTI MIGLIORABILE

8. EFFETTI DELLA VALUTAZIONE

Si sviluppano **AZIONI CONCRETE ED EFFICACI**, accompagnate da un crecente interesse dei diversi attori presenti nell'arena di policy.

Abstract - *A cura di* SIMONE COLOMBO

PUNTI DI RIFERIMENTO

- Struttura di valutazione di riferimento: National Audit Office (GB)
- Report di riferimento: *https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf*

➢ ***A cura di*** ASSERO Valeria, BARAZZETTA Claudio, BIANCHI Carlo, BISSANTI Gemma, CAVANNA Sara, COLOMBO Simone, MIDURI Miriana, SALA Martina

LE CARATTERISTICHE DEL N.A.O.

A cura di MARTINA SALA (matr. 951961)

LE CARATTERISTICHE DEL NAO:
LE ORIGINI E I RAPPORTI COL PARLAMENTO

LE ORIGINI

800 years of scrutinising the spending of public money

1314: First Auditor of the Exchequer

1559: Auditors of the Imprest established

1780: Commissioners for Auditing the Public Accounts appointed by statute

150 years of C&AG

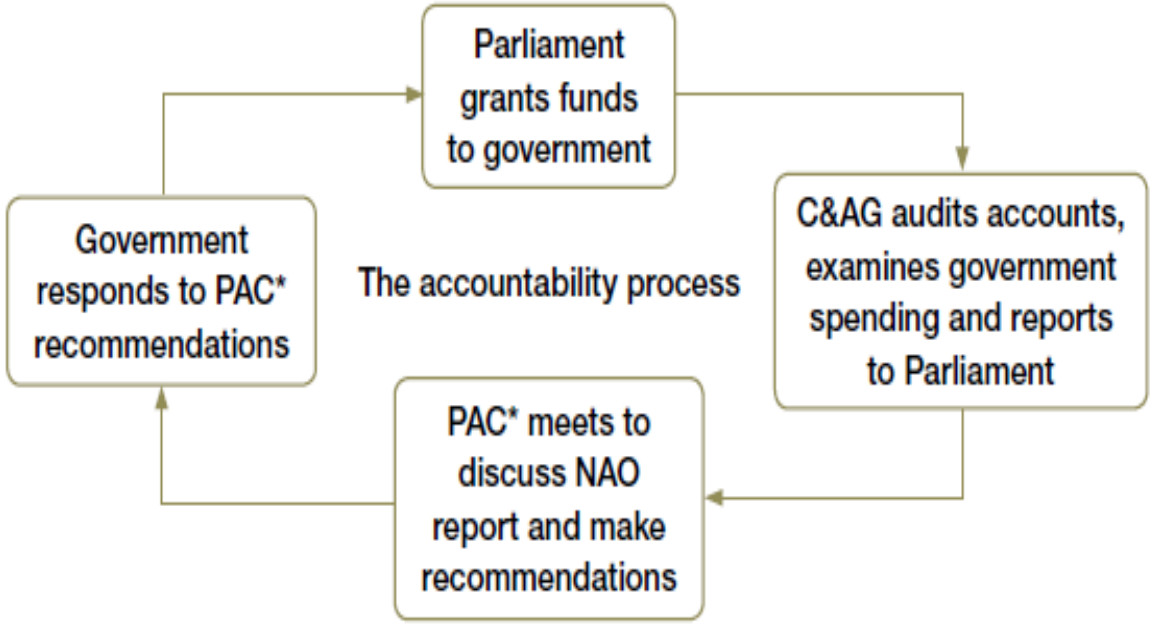
1866: Exchequer and Audit Departments Act requires all departments to produce annual accounts and established the position of Comptroller and Auditor General (C&AG), supported by an Exchequer and Audit Department (E&AD), staff by civil servants.

1983: National Audit Act established National Audit Office – independent of the civil service – and The Public Accounts Commission (TPAC).

Read more about the History of the NAO.

Fonte: NAO *(Posted on June 30, 2016 by Amyas Morse)*

I RAPPORTI COL PARLAMENTO



*Committee of Public Accounts

LE CARATTERISTICHE DEL NAO:
TIPOLOGIE DI INDAGINI ED ORGANIZZAZIONE INTERNA

TIPOLOGIE DI INDAGINI DEL NAO

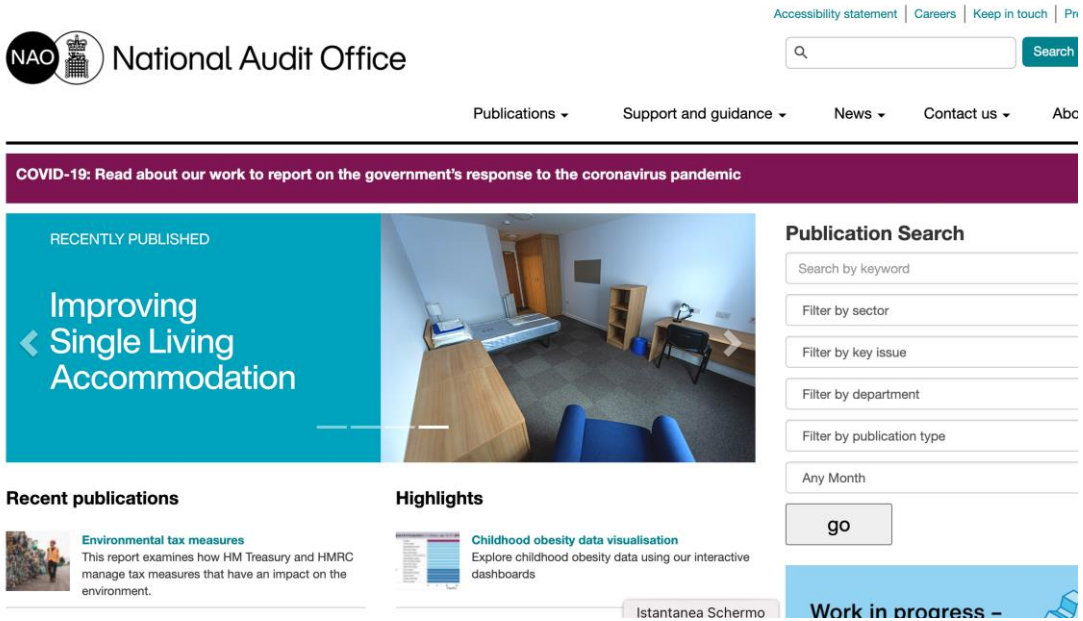
- Ci sono 5 aree di lavoro:
  1) FINANCIAL AUDIT
  2) VALUE OF MONEY
  3) INVESTIGATIONS
  4) SUPPORT FOR PARLIAMENT
  5) INTERNATIONAL

- L'obiettivo principale: creazione di Report in grado di valutare in modo autonomo e indipendente l'andamento di una Policy intrapresa dal governo in diversi settori per capire se i soldi pubblici vengono investiti nel modo corretto e fruttuoso da parte del governo (rapporto investimento – benefici).

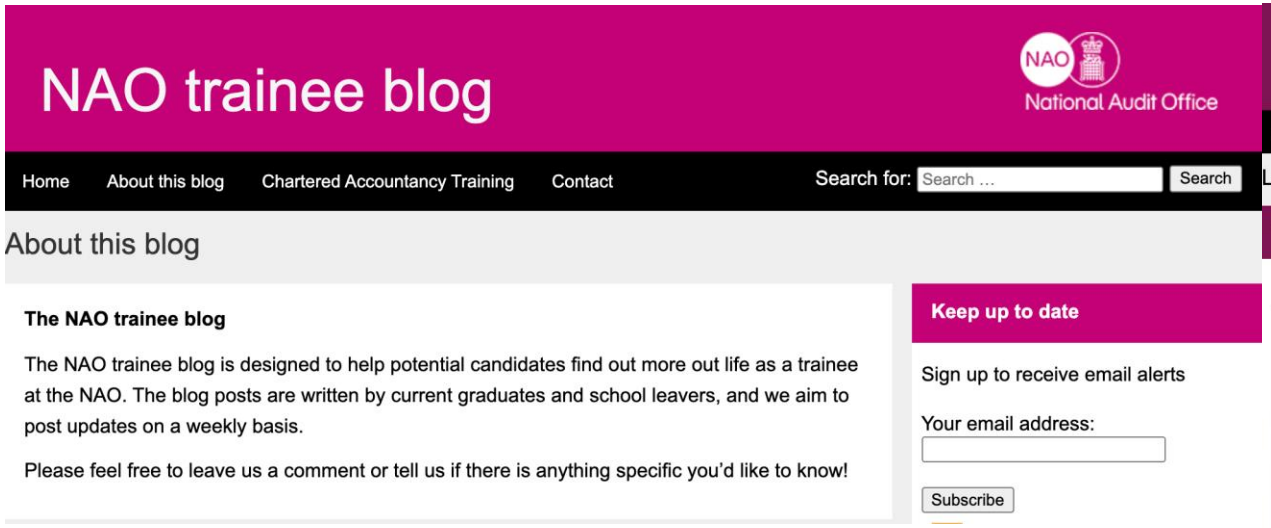
ORGANIZZAZIONE INTERNA

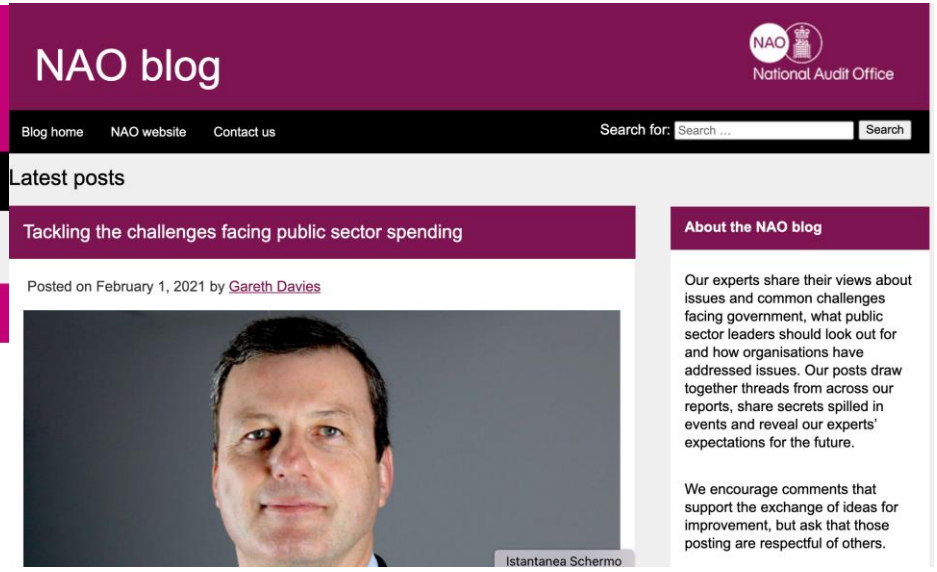
- La NAO presenta una struttura operativa molto ampia ed è composto da circa **800 analisti.**
- Al vertice della struttura interna vi è **il COMPTROLLER AND AUDITOR GENERAL (C&AG).**
- poi vi è un **CONSIGLIO DI AMMINISTRAZIONE**
- **un EXECUTIVE TEAM,**
- **un Presidente non esecutivo**
- **membri non esecutivi del consiglio e amministratori esecutivi.**
- Particolare attenzione ai giovani

LE CARATTERISTICHE DEL NAO:
IL SITO WEB

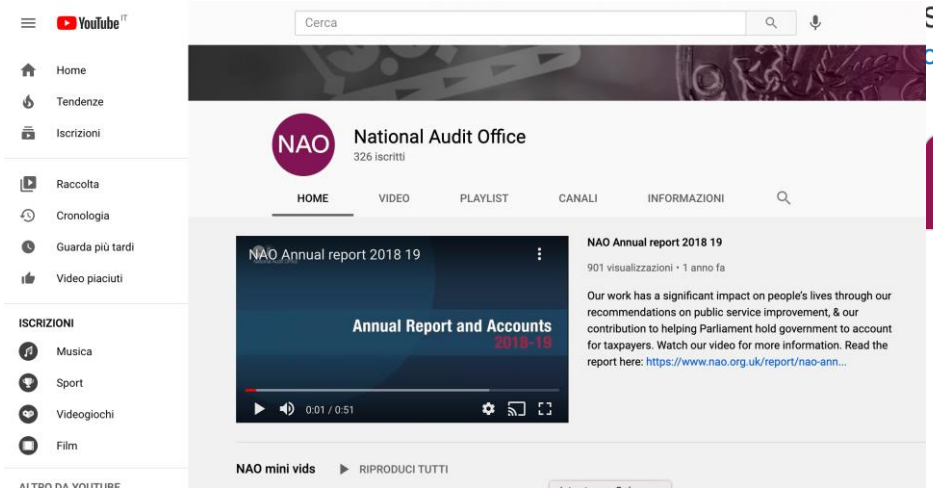


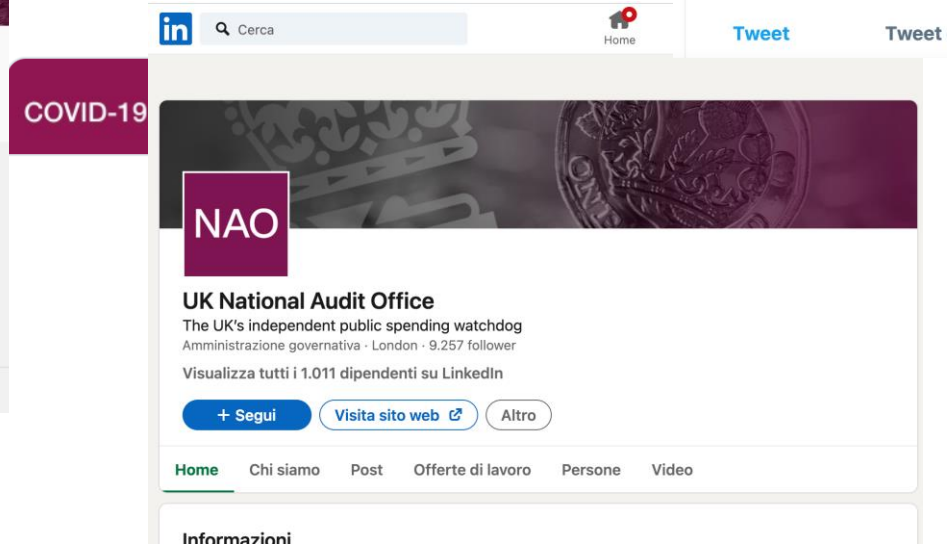
Fonte: National Audit Office (NAO)





LE CARATTERISTICHE DEL NAO:
I SOCIAL





Fonte: National Audit Office (NAO)

IN SINTESI

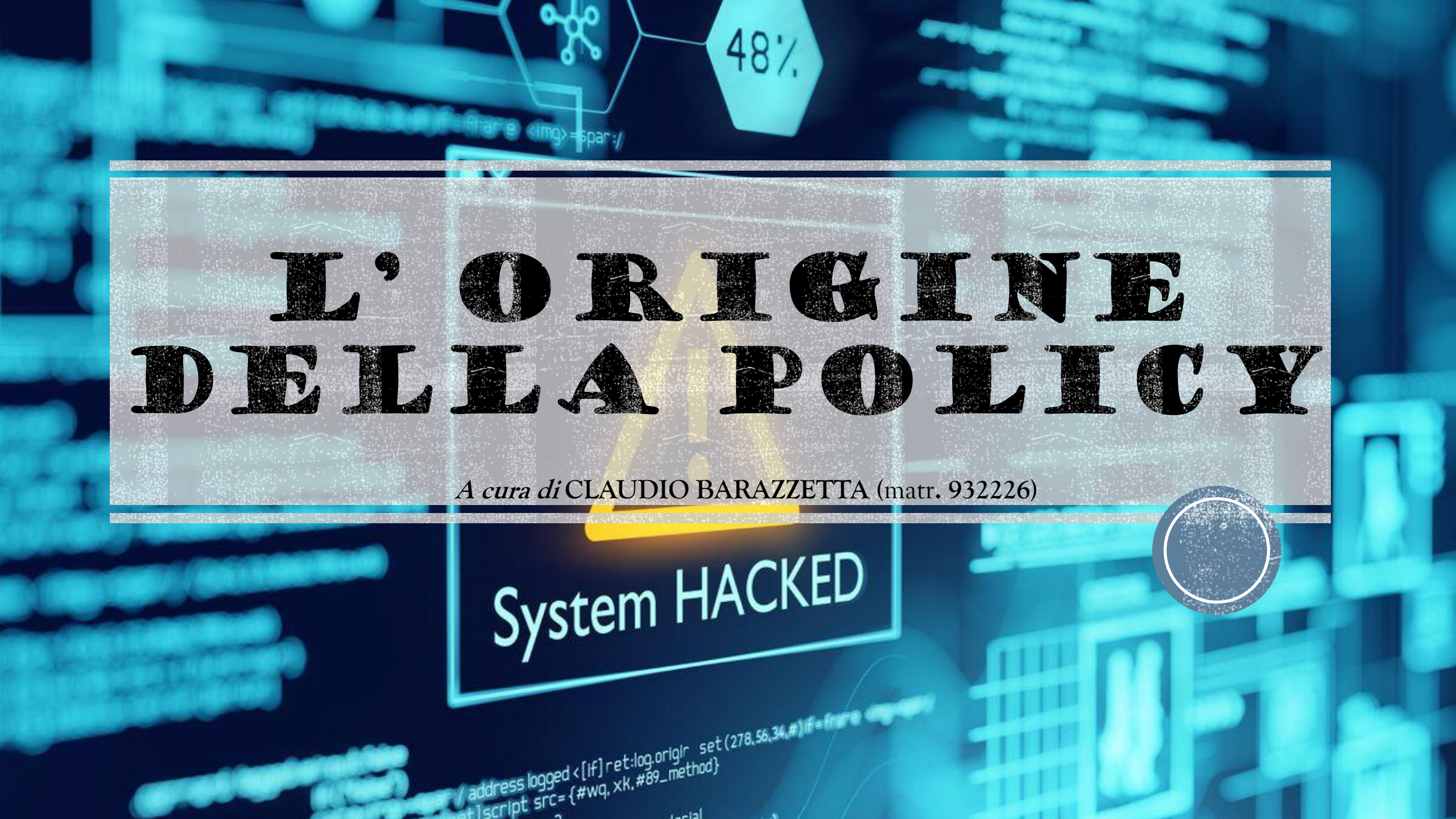
- Una storia che ha origine 800 anni fa
- Un interdipendente rapporto con il parlamento
- 5 aree di lavoro
- 800 analisti
- Creazione di report in grado di valutare una policy in modo indipendente
- Un sito chiaro ed interessante

FONTI

- https://www.public-audit-forum.org.uk/uk-members/national-audit-office
- https://www.nao.org.uk
- https://www.nao.org.uk/graduateblog/

L'ORIGINE DELLA POLICY

A cura di CLAUDIO BARAZZETTA (matr. 932226)



L'ORIGINE DELLA POLICY

IL PROBLEMA

1.

- Le imprese e i cittadini operano sempre più online per fornire vantaggi economici, sociali ecc, rendendo il paese sempre più dipendente da Internet
  → 1/8 del PIL UK deriva dall'economia digitale (2016);
- UK aspira a diventare leader mondiale nell'economia e nel governo digitali
  → collegamento sempre più forte dei servizi governativi e dell'amministrazione pubblica a Internet;
- Il 90% delle famiglie è connesso a internet
  → la più alta proporzione mondiale di individui connessi;
- Ruolo internazionale preponderante
  → ONU, NATO, Commonwealth…

2.

- 72% aziende UK segnalano almeno un attacco informatico – 9% più di un attacco giornaliero;
- Oltre 1100 attacchi informatici registrati dal NCSC (dal 10/2016);

3.

- Gli obbiettivi del 50% dei cyberattacks sono il governo, le società di telecomunicazioni, le organizzazioni della difesa nazionale e i siti accademici
- Il danno medio degli attacchi è di € 1.400 per le piccole aziende e di € 10.500 per le grandi aziende

4.

- 2023 → oltre 20 miliardi di dispositivi connessi a Internet – *Internet delle Cose*
- Elementi tradizionalmente non concepiti per Internet – elettrodomestici, veicoli – ora costruiti e progettati per essere connessi in rete senza standard di sicurezza comuni e in cui la sicurezza informatica potrebbe essere più debole dei sistemi digitali dedicati.

5.

L'intero sistema-paese è potenzialmente sempre più soggetto a cyberattacks che rappresentano *la minaccia più acuta e diretta alla sicurezza nazionale*

L'ORIGINE DELLA POLICY

COME? DOVE? QUANDO?

- 2010 → Il Cabinet Office UK valuta strategie e programmi centralmente gestiti per garantire protezione contro gli attacchi informatici
- 2011 → Adozione della prima National Cyber Security Strategy
- 2011 – 2016 → Implementazione del primo programma relativo alla National Cyber Security (NCSP1)
- 10/2016 → Istituzione del National Cyber Security Centre come Autorità tecnica del Regno Unito sulla sicurezza informatica, accorpando 4 enti pre-esistenti
- 2016 → Adozione della seconda National Cyber Security Strategy
- **2016 – 2021 → Implementazione del secondo Programma relativo alla National Cyber Security**

National Cyber Security Centre

Fonte: NAO

L'ORIGINE DELLA POLICY

COME? DOVE? QUANDO?

UK IS SECURE AND RESILIENT TO CYBER THREATS, PROSPEROUS AND CONFIDENT IN THE DIGITAL WORLD

Sfida complessa che richiede il coinvolgimento delle **imprese** e del **pubblico** per gestire la propria esposizione al rischio informatico

Ruoli e le responsabilità che gli **individui**, le **imprese**, le **organizzazioni** e il **governo** devono assumersi per assicurarsi che i loro sistemi siano sicuri

€ 2.000.000.000

(=1,9 miliardi di Sterline)

Budget di spesa

- 12/05/2017 → Attacco informatico tramite il virus WannaCry ai sistemi informatici del National Health Service **(caso studio)**
  - 1/3 delle amministrazioni del NHS vengono attaccate
  - 19.000 prenotazioni sanitarie vengono cancellate
  - Inadeguatezza delle amministrazioni contro eventuali attacchi informatici
- 06/2017 → Rapporto NAO sulle frodi informatiche evidenzia perdite stimate
  - € 11.500.000.000 per gli individui
  - € 165.000.000.000 per il settore privato

→ Il governo non dispone di meccanismo chiari per identificare, sviluppare e condividere buone pratiche per evitare attacchi informatici

L'ORIGINE DELLA POLICY

LE CONSEGUENZE

- Analizzare i dati e gli outcomes del NCSP
- Correggere l'attività del governo circa le azioni da intraprendere per migliorare la qualità della cybersecurity
- Implementare i buoni risultati del Programma 2016-2021 in ottica futura ponendo le basi per una strategia post 2021

- Rafforzare i 12 obiettivi strategici evidenziati dalla NCSS 2016-2021 in ottica intergovernativa (NCSC, Home Office, Department for Digital, Culture, Media & Sport, Cabinet Office, Foreign & Commonwealth Office) avendo come sfondo i temi della **Deterrenza**, della **Difesa** e dello **Sviluppo**
- Incentivi alle imprese per investire nel settore informatico migliorando gli standard di sicurezza informatica in tutta l'economia
  → aumento dei finanziamenti per finanziare i NCSP
- Stabilire le aree del NCSP di maggiore impatto, le priorità più elevate, superare le criticità
  → ridistribuire il budget secondo un preciso business-case
- Implementare confronti e sinergie con altri dipartimenti governativi
  → comprendere le loro priorità di sicurezza informatica
- Definire una futura divisione del lavoro
  → quali attività devono essere finanziate centralmente, quali le responsabilità del settore privato e quali le attività proprie dei dipartimenti
- Rapida evoluzione della cybersecurity
  → programmi più brevi per essere più reattivi ai cambiamenti

IN SINTESI

2

- L'intero sistema-paese è potenzialmente sempre più soggetto a cyberattacks che rappresentano *la minaccia più acuta e diretta alla sicurezza nazionale*
- Emerge che il governo non dispone di meccanismo chiari per identificare, sviluppare e condividere buone pratiche per evitare attacchi informatici
- Emerge l'esigenza di una rapida evoluzione della cybersecurity con programmi più brevi per essere più reattivi ai cambiamenti

FONTI

- **NAO – Progress of the 2016-2021 National Cyber Security Programme** https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf

STRUMENTI, FINANZIAMENTI, STRUTTURA

A cura di SARA CAVANNA (matr. 934037)

STRUMENTI, FINANZIAMENTI, STRUTTURA
IL QUADRO NORMATIVO E GLI INDIRIZZI DEL GOVERNO

ACT

- Intelligence Services ACT 1994 (abbreviato ISA)
- Security Service Act 1989 modificato nel 1996
- Investigatory Powers Act 2016.
- Digital Economy Act 2017
- Data Protection Act 2018 (abbreviato in DPA)
- Regulation of Investigatory Powers Act 2000 (abbreviato in RIP o RIPA)
- Freedom of Information Act 2000 (abbreviato in FOIA)

REGULATIONS

- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Environmental Information Regulations 2004
- The Network and Information Systems Regulations 2018
- The Cyber-Attacks (Asset-Freezing) Regulations 2019
- The Digital Economy Act 2017 Regulations 2020

GLI INDIRIZZI STRATEGICI DEL GOVERNO

- Si tratta delle strategie programmatiche adottate dal governo britannico per rendere la Gran Bretagna sicura e resiliente nel cyberspazio.
  - **National Cyber Security Strategy 2016 to 2021** https://www.gov.uk/government/cyber-security
  - **UK Digital Strategy (marzo 2017)** https://gds.blog.gov.uk/category/digital-strategy/
  - **Industrial Strategy (novembre 2017)** https://www.gov.uk/government/news/the-industrial-strategy-in-action

STRUMENTI, FINANZIAMENTI, STRUTTURA

I FINANZIAMENTI

- La National Cyber Security Strategy 2016 prevede un finanziamento complessivo per la Strategia di 1,9 miliardi di sterline, di cui 1,3 miliardi per il Programma.
- Finanziamenti Programma per il quinquennio 2016-20121 effettivamente spesi alla data di stesura del Report del NAO

TRIENNIO 2016-2018:

Spesi 652 miloni di sterline, pari al 50,15% del totale

TRIENNIO 2019-2021:

Spesi 649 miloni di sterline, pari al 49,85% del totale

- L'HM Treasury ha approvato i finanziamenti del programma **prima** che la strategia fosse sviluppata.
- Il Dipartimento **non ha valutato** se il finanziamento, che era già stato stabilito da HM Treasury nel 2015, sarebbe stato sufficiente per soddisfare i risultati strategici. Altresì, da allora non ha più intrapreso alcun lavoro per valutare se i finanziamenti fossero sufficienti per realizzare la Strategia.

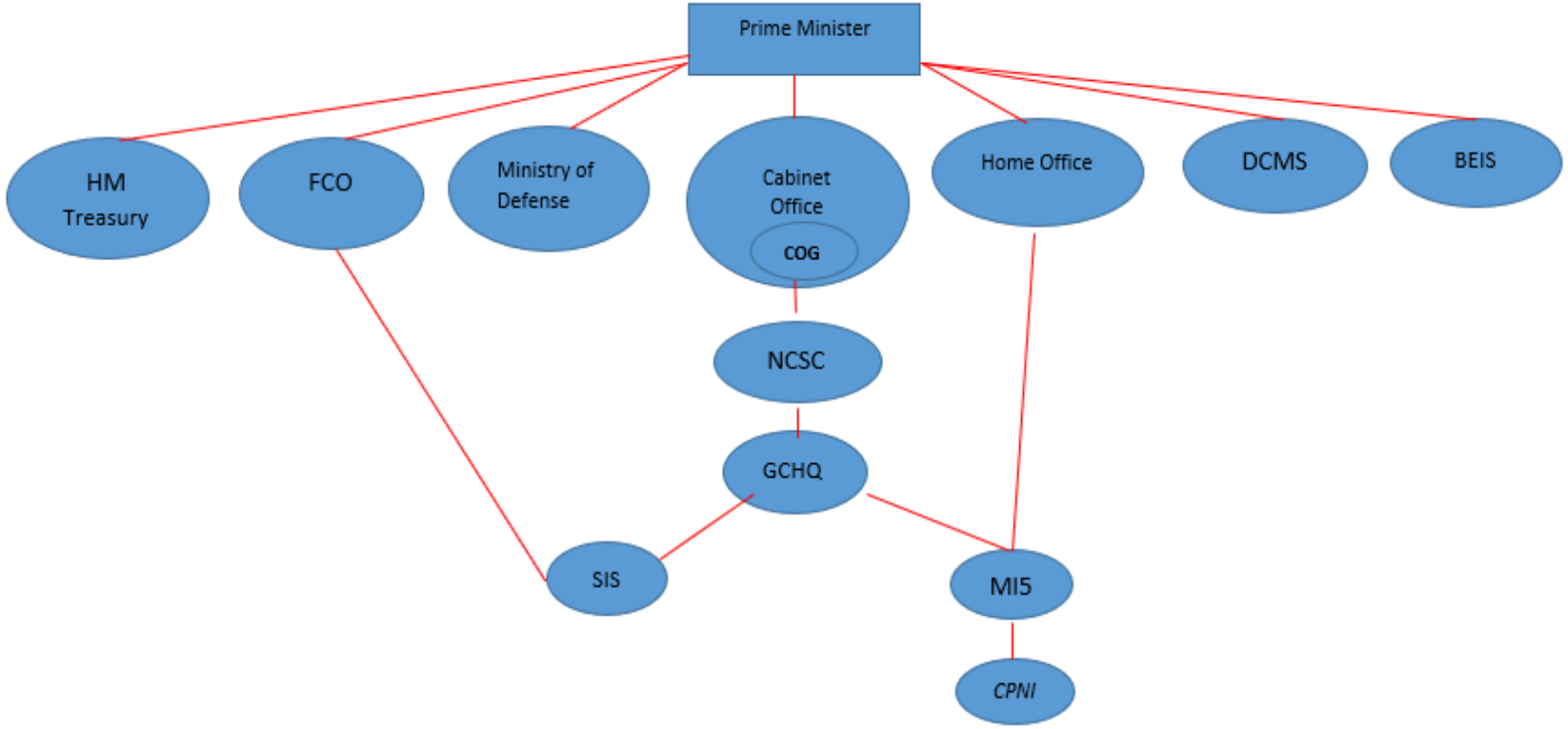
- **Solo il 31 maggio 2018** il Dipartimento ha formalmente **autorizzato** le strutture dipartimentali designate **a spendere** fino al 90% delle assegnazioni esistenti, poiché le discussioni non erano ancora state risolte. Almeno quattro dipartimenti guida hanno ritardato o ridotto parte del loro lavoro a causa dell'incertezza.
- Ammonta a £ 169 milioni (pari al **37% del finanziamento)** le risorse destinate al Programma che sono state **prestate** o **trasferite** nei primi due anni per sostenere **altre attività** (finanziamento per la lotta al terrorismo, Foxhound e Verify)

STRUMENTI, FINANZIAMENTI, STRUTTURA
LA STRUTTURA DELLA CYBER SECURITY NAZIONALE

- Il Cabinet Office è il responsabile del coordinamento dell'attuazione della Strategia di CyberSecurity adottata dal Governo per il quinquennio 2016-2021

- Il buon esito dell'attuazione della Strategia dipende però dalla consegna dei progetti del Programma da parte di altri Dipartimenti, dai contributi di organizzazioni e individui esterni al proprio diretto controllo. Il Cyber Oversight Group è la sottostruttura designata a supervisionare sia la Strategia che il Programma.

Fonte: elaborazione propria



Abbreviazioni e Sigle

FCO (Foreign, Commonwealth and Development Office),
COG (Cyber Oversight Group),
DCMS (Department for Digital, Culture, Media & Sport),
BEIS (Department for Business, Energy & Industrial Strategy),
NCSC (National Cyber Security Centre),
GCHQ (Government Communications Headquarters),
SIS o MI6 (Secret Intelligence Service),
MI5 (Security Service) e CPNI (Centre for the Protection of National Infrastructure).

IN SINTESI

3

- Diversi strumenti normative(Law e Regulation)
- La National Cyber Security Strategy 2016 prevede un finanziamento complessivo per la Strategia di 1,9 miliardi di sterline, di cui 1,3 miliardi per il Programma.
- Il Cabinet Office è il responsabile del coordinamento dell'attuazione della Strategia di CyberSecurity, tuttavia il buon esito dell'attuazione della Strategia dipende dalla consegna dei progetti del Programma da parte di altri Dipartimenti, dai contributi di organizzazioni e individui esterni al proprio diretto controllo.

FONTI

- **National Cyber Security Centre:** https://www.ncsc.gov.uk
- **UK Statute Law Database:** https://www.legislation.gov.uk/
- **Royal United Services Institute:** https://rusi.org/sites/default/files/20190627_the_uk_cyber_strategy_web
- **House of Commons & Defence Committee:** https://committees.parliament.uk/publications/2265/documents

IMPLEMENTAZIONE: POLICY TOOLS, ATTORI E INIZIATIVE

A cura di CARLO BIANCHI (matr. 951515)

L'IMPLEMENTAZIONE

QUALI POLICY TOOLS SI SONO SCELTI PER RISOLVERE IL PROBLEMA?

- Il governo britannico affida ai singoli dipartimenti governativi e agli enti pubblici la responsabilità della salvaguardia delle proprie informazioni.

- Dal 2010 però il governo ha deciso di adottare strategie e programmi guidati centralmente per garantire che il Regno Unito gestisca efficacemente e in maniera uniforme in tutti i dipartimenti la propria esposizione ai rischi legati alla sicurezza informatica.

- Il **Cabinet Office** guida questo lavoro, attraverso l'elaborazione delle National Cyber Security Strategies, pubblicate nel 2011 e nel 2016; inoltre ha provveduto alla creazione di programmi nazionali separati per la sicurezza informatica progettati per aiutare a realizzare ciascuna strategia tra il 2011-2016 e il 2016-2021.

- La strategia per il **quinquennio 2016-2021 si basa su 3 pilastri fondamentali, sviluppati a loro volta in 12 risultati strategici da raggiungere: Scoraggiare gli attacchi informatici, difendersi contro l'evoluzione delle minacce informatiche, sviluppare l'industria della cyber security.**

- Al fine del raggiungimento dei risultati prefissati dalla strategia il programma nazionale per la sicurezza si è prefissato 12 obiettivi, affidati a 5 dipartimenti separati.

L'IMPLEMENTAZIONE

QUALI ATTORI SI SONO ATTIVATI E QUALI SI SONO OPPOSTI?

- **Gli attori coinvolti nello sviluppo di questa policy sono diversi.**

- Il primo è il governo britannico, responsabile della supervisione della Strategia e del Programma, e i cinque dipartimenti responsabili del raggiungimento degli obiettivi del Programma.

- Il secondo attore è il **National Cyber Security Centre(NCSC)**, l'autorità responsabile della cyber security nel paese,creata nel 2016 dalla fusione di quattro autorità pre esistenti. Gli obiettivi dell'NCSC sono di aumentare la sicurezza informatica del paese attraverso lo studio e la condivisione di nuove conoscenze, e collaborare con aziende pubbliche e private per migliorare la loro sicurezza al fine di ridurre i rischi di attacchi.

- Esso nasce inizialmente come parte del **Government Communications Headquarters' (GCHQ).** Tuttavia, al momento della sua istituzione, vi è un forte contrasto tra questi due organismi, a causa delle diverse funzioni che rivestivano, con un ruolo di organismo aperto che fornisce consulenza e guida il primo, e un' organizzazione di intelligence segreta il secondo.

- Tuttavia l'iniziale creazione dell'NCSC all'interno di un'altra organizzazione gli ha permesso di poter essere operativo in poco tempo, grazie al trasferimento di più di 600 dipendenti GCHQ quando è stato aperto e all'utilizzo delle strutture già esistenti per aiutare la configurazione Progetti finanziati dal programma entro il primo anno.

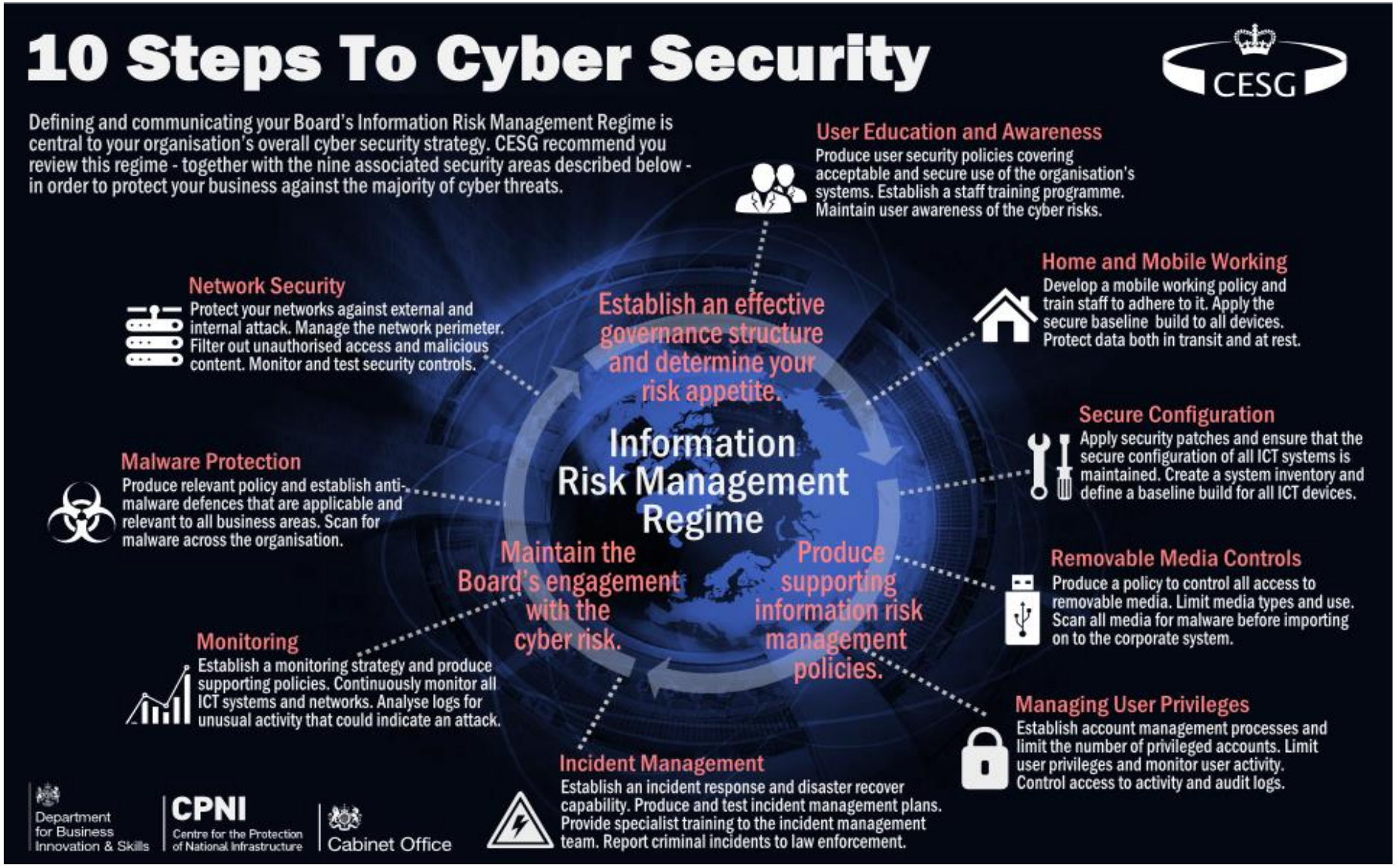
L'IMPLEMENTAZIONE

QUALI INIZIATIVE SONO STATE ADOTTATE PER FAR FUNZIONARE LA POLICY O PER OSTACOLARLA?

- Per far funzionare questa policy sono stati adottati diversi strumenti tra cui: la creazione del NCSC e la creazione nel 2020 di un nuovo organismo, la **National Cyber Force**, gestita dal dipartimento della difesa e dal Government and Communications Headquarters.
- L'obiettivo principale dell'NCF sarà individuare, interrompere e persino distruggere i sistemi di comunicazione dei soggetti che rappresentano una minaccia per la sicurezza.
- La Forza monitorerà le minacce alla sicurezza informatica sia locali che globali e il mandato dell'organizzazione
- Comprenderà anche il sostegno alle operazioni militari attualmente in corso. Un'altra tattica che l'NCF utilizzerà è quella di adottare un approccio di scienza comportamentale nel tentativo di comunicare con gli aggressori per scoraggiarli dall'attaccare.
- Un altro organismo lanciato dal governo è il **Cyber Security Council** , che ha lo scopo di promuovere le prospettive di lavoro qualificato in tutto il paese fornendo lavoratori una chiara tabella di marcia per una carriera nella sicurezza informatica e concentrarsi sull'aumento del numero e della diversità delle persone che entrano nella professione.
- L'organismo lavorerà con le scuole di formazione per accreditare corsi e qualifiche e fornire ai datori di lavoro le informazioni e la fiducia di cui hanno bisogno per assumere in modo efficace per garantire la loro capacità informatica.

L'IMPLEMENTAZIONE

QUALI INIZIATIVE SONO STATE ADOTTATE PER FAR FUNZIONARE LA POLICY O PER OSTACOLARLA?



Fonte: NAO

IN SINTESI

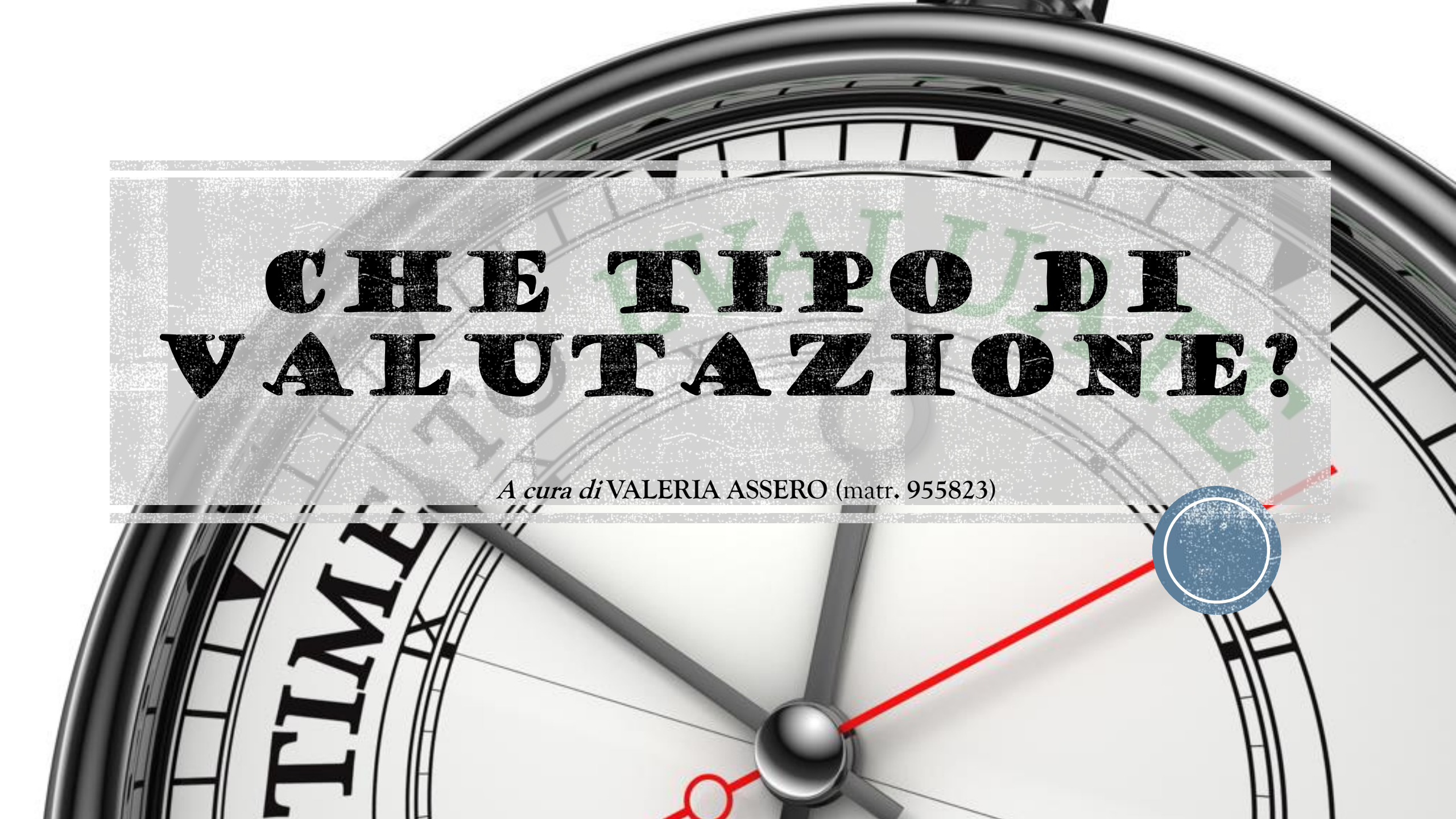
- 3 pilastri fondamentali e 12 obiettivi
- 2 attori principali: il governo e il National Cyber Security Centre(NCSC),
- Per far funzionare questa policy sono stati adottati diversi strumenti tra cui: la creazione del NCSC e la creazione nel 2020 di un nuovo organismo, la National Cyber Force, gestita dal dipartimento della difesa e dal Government and Communications Headquarters
- Un altro organismo lanciato dal governo è il Cyber Security Council
- Un' implementazione "multipolare"

FONTI

- **NAO – Progress of the 2016-2021 National Cyber Security Programme** https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf
- https://globalriskinsights.com/2021/01/uk-government-announces-new-national-cyber-force/
- https://www.businesscloud.co.uk/news/uk-cyber-security-council-launched-by-government/

CHE TIPO DI VALUTAZIONE?

A cura di VALERIA ASSERO (matr. 955823)



CHE TIPO DI VALUTAZIONE?

IL DISEGNO DI RICERCA

I PUNTI PIU' IMPORTANTI

- Nonostante le perdite economiche a causa delle frodi in Inghilterra fossero state stimate nel 2016 per un totale 10 miliardi di sterline per i cittadini e di 144 miliardi per il settore privato, **il governo non disponeva** di un **meccanismo chiaro per identificare, sviluppare e condividere buone pratiche per evitare che le persone diventassero vittime del web**.

- Il National Audit Office del Nao nel suo report del 2016-2021 Sicurezza informatica nazionale ha elaborato i dati raccolti in merito e stilato le raccomandazioni e valutazioni sul sistema informatico del Regno Unito→ «**sentiment analysis**»

  - Caso mondiale «**WannaCry2017**».
  - L'ambizione del Governo **UK** di essere **un leader mondiale nel governo digitale** e di **cementificare** questa sua **posizione**
  - **Combattere** le **frodi on line** ai danni dei cittadini.
  - **Partnership con l'industria della difesa informatica attiva con le altre Nazioni** contro gli attacchi di phishing e malware su larga scala.
  - **Collaborazione** in ottica di cybersecurity tra **Pubblico e Privato**.

HEALTH SERVICE HACKED

Hospitals to struggle for days

Doctors have revealed an MRI scanner went down with an anaesthetised child inside

Malicious software shut down NHS computers with a message demanding $300 in bitcoin

Fonte: https://www.thetimes.co.uk/article/nhs-cyberattack-bitcoin-wannacry-hospitals-to-struggle-for-days-k0nhk7p2b

WannaCry, quanto rischia l'Italia? Poco, visto che l'informatica non funziona

Fonte: https://www.ilfattoquotidiano.it/2017/05/16/wannacry-quanto-rischia-litalia-poco-visto-che-linformatica-non-funziona/3588747/

QUANDO E PERCHÈ VIENE AVVIATA LA RICERCA?

QUANDO INIZIA L'ATTIVITA' DI RICERCA IN MERITO DEL NAO?

- Il precedente lavoro del Nao *Rapporto Online fraud 2017* aveva già identificato quanto Internet fosse importante per il governo e la società, ma anche l'impatto su di essi degli attacchi informatici. Nello stesso rapporto era stato osservato che l'82% della popolazione adulta del Regno Unito ha utilizzato Internet quasi ogni giorno e che più della metà delle frodi veniva commessa online. Con l'indagine 2018 a seguito del WannyCry2017 il Nao sottolinea anche l'esistenza di un ulteriore rapporto del **Dipartimento della Salute e dell'Assistenza Sociale** sull'incidente informatico del maggio 2017 e aveva pure osservato che nessuna delle 80 organizzazioni colpite dall'attacco informatico non aveva applicato l'ultimo patch di aggiornamento consigliata→ **nonostante avesse avuto specifiche raccomandazioni → considerare il fatto** come ulteriore campanello d'allarme di **un problema in generale ampliamente sottovalutato** e nello specifico identificativo dell' **assenza di scelte di policy adeguate al problema.**

PERCHE' VIENE AVVIATA LA RICERCA?

- **L'indagine 2018 sull'attacco informatico WannaCry di maggio 2017** ha rilevato che la Gran Bretagna è stato uno dei Paesi più colpiti, in termini di conseguenze, dove il virus informatico ha mandato **in tilt diversi ospedali**. Questo è stato possibile, proprio perché nelle strutture ospedaliere del Regno Unito **ci sono ancora molte migliaia di computer con Windows XP** più facilmente **attaccabili**.
- **Il rapporto del NAO**, quindi, **ha scoperto che l'allora Dipartimento per la Salute e i corpi del suo braccio non sapevano se le organizzazioni locali** fossero **adeguatamente preparate** per un **attacco informatico sebbene informate preventivamente dei rischi che correvano.**

LA DOMANDA DI RICERCA
UNA VALUTAZIONE IN ITINERE ED EX-POST

- Vi è stata una **riduzione delle frodi** on line e degli attacchi alla Cybersicurity nel sistema informatico del Regno Unito? Quest'ultimo è effettivamente **riuscito a imporsi come leader in questo campo** per la sicurezza informatica globale?
  - **Output**: numero di controlli eseguiti nei sistemi informatici del pubblico e delle aziende private;
  - **Outcome**: variazioni nella quantità dei cyberattacchi e nelle frodi informatiche;
  - **Impatto**: quanta parte delle variazioni è dovuta alla policy in campo di Cybersicurity adottata dal Regno Unito?

- La valutazione d'impatto deve considerare le possibili cause interne o esterne all'intervento.
  Possibili cause interne: l'output (controlli, informazioni agli utenti..) → secondo raccomandazioni del NAO sono migliorabili.
  1) Una **maggiore capacità di informare** da parte del Dipartimento **sia nel privato che nel pubblico** sui pericoli dei **cyberattacchi informatici**.
  2) Rafforzare la **pressione** su di questi **affinché si adeguino alle linee guida costituita dai 12 punti strategici** facendo monitoring.
  3) Sia nel pubblico che nel privato **continua a mantenersi una sottovalutazione del problema** che fa si che i loro sistemi informatici non siano al passo della tecnologia rendendoli così più vulnerabili dagli attacchi di gruppi informatici sempre più sofisticati.
  4) La Tesoreria presta il 37% dei finanziamenti destinati ai primi due anni del programma per le attività antiterrorismo e sicurezza nazionale → ha ritardato il lavoro sui progetti come attività di lavoro per comprendere la minaccia informatica.
  5) Vengono stanziati per il 2021 342 milioni di sterline che sono il doppio della somma erogata per il primo anno.

- **Possibili cause esterne non aggredibili dall'intervento pubblico**: manca un'effettiva collaborazione tra settore Pubblico e Privato.

CHE TIPO DI VALUTAZIONE?

Valutazione ex post o 'sommativa' per riassume dopo un congruo periodo, per capire se la politica ha funzionato o no	*Risultati*
Complessivamente, le risorse sono state adeguate?	✗
L'uso che ne è stato fatto ha rispettato il criterio di efficienza?	✗
Ci prodotti e servizi sono stati effettivamente forniti?	✓
Ci sono stati scostamenti dalle previsioni?	✓
Qual è oggi lo stato del problema iniziale?	✓
Quali valutazioni ne danno gli interessati?	✗
I cambiamenti di lungo periodo si sono verificati?	✗
Sono intervenuti fattori non previsti?	✓

IN SINTESI

5

- L'ambizione del Governo UK di essere un leader mondiale nel governo digitale e di cementificare questa sua posizione fa sorgere l'eseigenza di migliorare i sistemi di sicurezza informatica. Ecco che qui entra in gioco l'attività del NAO con le sue raccomandazioni e valutazioni in merito.
- Due tipi di valutazione:
  - Una valutazione *ex post* per gli obiettivi portati a termine con il prima programma NCSP1 terminato nel 2016.
  - Nel secondo Programma di sicurezza nazionale 2016-2021 il NAO opera con suggerimenti per risolvere il problema sulla sicurezza informatica prefigurato come in costante evoluzione con una valutazione per questo *in itinere*.

FONTI

- **NAO – Progress of the 2016-2021 National Cyber Security Programme** https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf

L'ANALISI DEL REPORT

A cura di MIRIANA MIDURI (matr. 961873)

L'ANALISI DEL REPORT
I METODI DI RICERCA

- **In tutte le fasi** vengono effettuate interviste ad alti funzionari del Dipartimento e di altri dipartimenti governativi e fornite raccomandazioni molto spesso disattese.

NON RICORRENTI

I

- Esame strategie, linee guida e documenti del governo sulla sicurezza, da enti del settore, da società di ricerca;
- incontri figure del settore per visione esterna.

II

- Analisi rapporti sulle prestazioni non pubblicati e sui progressi dei singoli dipartimenti;
- analisi finanziaria dati forniti dal Dipartimento;
- Esame rapporti consiglio di amministrazione e NSC Review 2018;
- Avvio di nuovi progetti di successo
- Riesame dei programmi per valutazione qualità della gestione.

III

Analisi dati sulle prestazioni.

RICORRENTI

I-II

Partecipazione a briefing del NCS Center

I-IV

Partecipazione a eventi di settore;

III-IV

Esame documenti pubblicati e non;

L'ANALISI DEL REPORT
GOVERNMENT E POLICIES

- valutazione insufficiente del finanziamento HM Treasury
- periodo di ri-profilazione non utilizzato
- Nessuna informazione dai dipartimenti sulle prestazioni.
- Mancanza di un business case complessivo
- Incapacità di identificare, sviluppare e condividere buone pratiche tra la popolazione

➢ **Conseguenze sul programma**

dati storici limitati, mancanza di misure quantitative, linee di base inadeguate per l'allocazione delle risorse, priorità e misurazione efficace dei progressi.

➢ **Strategia 2016**: aiuti alle imprese, istituzione NCS e Programma Active Cyber Defense.

➢ **Trimestre 2018-2019:** Rapporto NCS Review, riesame capacità sicurezza nazionale, Rapporto Comitato congiunto sulla strategia di sicurezza nazionale e valutazione dei dipartimenti principali dello stato di avanzamento dei progetti del programma.

➢ **Progetti fuori pista:** nuovi consigli di amministrazione; reclutamento 3 rappresentanti del settore della sicurezza informatica; società di sicurezza all'estero e sviluppo professionisti della sicurezza informatica nel governo.

Frodi

2017 Annual fraud indicator

Rischio di un cyber attacco

2018 Government survey of cyber security breaches.

L'ANALISI DEL REPORT
AMPIEZZA DELLE EVIDENZE: I RISULTATI

PROGRESSI DEI MACRO OBIETTIVI:
DETER, DEFENDER, DEVELOP

- Il **Dipartimento** ha sviluppato:
  - Sistemi di rilevazione dei criminali informatici con l'intelligence e la sicurezza informatica delle forze dell'ordine;
  - Un programma informatico offensivo nazionale contro il terrorismo riducendo le capacità Daesh in Siria e Iraq;
  - Politica finalizzata per aumentare il costo delle attività informatiche maligne.
  - Gestione incidenti informatici e riduzione danni ad organizzazioni e cittadini con l'esperienza del NCSC e del National Crime Agency.

Companies

50% ha competenze tecniche di base;

27% ha una politica formale di sicurezza informatica;

36% vittima di attacco informatico adotta misure preventive o protettive.

Human capital

17 università accreditamento NCSC;

istituti di ricerca dedicati.

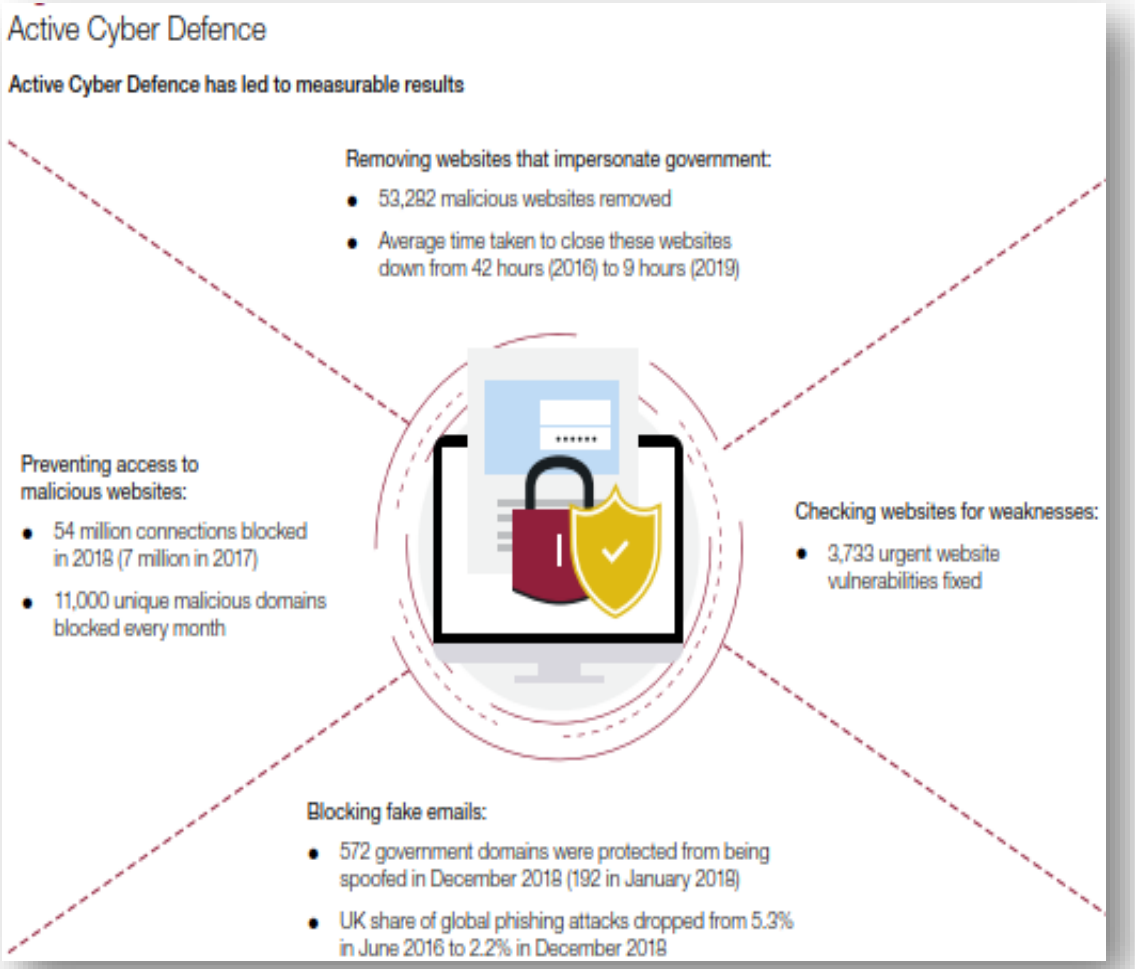
Active Cyber Defence

L'ANALISI DEL REPORT
AMPIEZZA DELLE EVIDENZE: I RISULTATI

- **Il National Cyber Security Center**, un'autorità tecnica sulla sicurezza informatica, ha affrontato più di 1.100 incidenti di sicurezza informatica in UK con l'Active Cyber Defense Programme

  - **L'ACD** inizialmente era **destinato al settore pubblico garantendo interventi e servizi gratuiti di sicurezza o mitigazione,** incoraggiargiando i siti di hosting a rimuovere contenuti dannosi, rendere difficile ai criminali la creazione di false email, che sembrano provenire da indirizzi affidabili, e verificare la sicurezza dei siti Web.

  - L'estensione dell''ACD al settore privato ha ridotto l'impatto dei cyber-attack e degli attacchi di phishing provenienti dal UK e **la riduzione della quota del globale dal 5,3% al 2,2% in due anni.**



Fonte: National Audit Office analysis of National Cyber Security Centre documentation

IN SINTESI

- Presenza di diversi metodi di ricerca, alcuni ricorrenti nel corso del report e delle indagini del NAO; altri *ad HOC*
- Companies, Human Capital, Active Cyber Defence

FONTI

- **NAO – Progress of the 2016-2021 National Cyber Security Programme** https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf

METAVALUTAZIONE

A cura di SIMONE COLOMBO(matr. 957819) & DEL GRUPPO

METAVALUTAZIONE
CARATTERISTICHE GENERALI

- L'analisi di un progetto di implementazione della Cyber Security è in parte in itinere, in quanto l'NCSP 2 è iniziato nel 2016 e si concluderà a marzo di quest'anno; tuttavia, **l'analisi non è totalemente in itinere in quanto all'interno del report si fa riferimento a Leggi, budget e valutazioni già approvate: si parla del NCSP 1 dandone un giudizio e una valutazione di efficienza EX POST.**

- **Emergono molti punti di miglioramento rispetto alla politica analizzata:**
  - **Il NAO sottolinea l'importanza di un cambiamento per i programmi futuri di Cyber Security in linea con i cambiamenti sociali, economici, scientifici e culturali sul tema che è sempre in divenire per via delle nuove scoperte nel campo.** Il cambiamento è altresì funzionale al fatto che i criminali informatici utilizzano tecniche sempre più sofisticate e meno note, tanto che il dipartimento per la sicurezza informatica fatica a stare al passo con questi cambiamenti.

- **Il report punta sulla trasparenza e sottolinea imparzialità di giudizio**, infatti:
  - Emerge un overwiev d'insieme: si dà peso alla maggiore sicurezza informatica derivante dal buon esito del Programma, ma anche al fatto che, con la messa in atto del programma, si avrà un aumento del capitale umano coinvolto insieme ad una maggiore attenzione allo sviluppo della ricerca scientifica sul tema.
  - Emerge continuità tra i due programmi avviati: **NCSP1 e NCSP2**

METAVALUTAZIONE

GRADO DI CHIAREZZA E LEGGIBILITA'

- **Il Report che abbiamo scelto risulta chiaro e leggibile nel complesso**. Tuttavia, a volte, le informazioni generali vengono ripetute creando una sorta di rindondanza.
- Presenta l'utilizzo di **elenchi puntati, tabelle, grafici e schemi** riassuntivi che rendono la valutazione chiara e scorrevole, mettendo in risalto i punti chiave che vengono espressi anche all'inizio dell'elaborato.
- I **key point** inseriti all'inizio forniscono una visione immediata e completa sia sul tema sia sulle analisi effettuate.

- Il report presenta una **chiara divisione del lavoro** e presentazione dei risultati e delle criticità emerse.
  - Vi sono ***4 parti***
    - I Approccio del governo alla sicurezza informatica
    - II Gestione del national cyber security program
    - III Progressi di attuazione del programma
    - IV Progetto fino al 2021 e futuro
  - e ***3 appendici***
    - I Come lavorano al NAO
    - II Dati e basi d'analisi
    - IIIValutazione di dipartimento

- **Chiarezza del tema affrontato** e delle sfaccettature date ad esso.
- Inoltre, la **presenza di un «cappello introduttivo»**, in cui si ha la presentazione del Watchdog e dei risultati, **contribuisce ad inquadrare il lavoro e a comprendere a pieno ciò che il NAO vuole analizzare** (rapporto costi-efficacia dei programmi di implementazione della sicurezza informatica).
- Le appendici e i dati raccolti contribuiscono ad accentuare **l'esigenza di trasparenza** del NAO che esprime chiaramente in che modo è giunto alle conclusioni del report (interviste ecc. ecc.).

METAVALUTAZIONE
I PUNTI DI FORZA E DEBOLEZZA DELLE CONCLUSIONI

- Vi è una **chiara descrizione del problema degli attacchi informatici** → Il Regno Unito che vuole diventare leader nell'ambito della digitalizzazione e della diffusione di internet e delle tecnologie→ Nel Repoty vi sono tutti i riferimenti a dati e leggi generali.
- Alcuni obiettivi si stimano realizzabili entro il 2021: **solo 3 su 12 obiettivi sono stati effettivamente realizzati, il resto degli obiettivi del programma 9 sono realizzati all'80%** con particolare attenzione alle infrastrutture nazionali critiche per la cyber security.
- Le spiegazioni nel report entrano in profondità **soprattutto riguardo i soldi spesi e quanto si riceve dal programma in termini di implementazione della sicurezza**, c'è ancora molta strada da fare ma si sono fatti dei miglioramenti.

Figure 6
The Department's February 2019 assessment of delivery against the Programme's objectives

Three objectives are assessed as having all their projects on track. All the other lead departments assessed their projects as at least 80% on track apart from Critical National Infrastructure

Objective	Lead Department	Programme progress
1 Understanding the threat	NCSC	🟡
2 Cybercrime	Home Office	🟡
3 Incident Management	NCSC	🟢
4 Active Cyber Defence	NCSC	🟢
5 Secure by Design	DCMS	🟡
6 Cyber Resilient Government	Cabinet Office	🟡
7 Wider Economy and Society	DCMS	🟡
7.1 Critical National Infrastructure	Cabinet Office	🔴
8 Growth	DCMS	🟡
9 Skills	DCMS	🟡
10 Research and Innovation	DCMS	🟡
11 Science and Technology	DCMS	🟡
12 International	FCO	🟢

🔴 Fewer than 80% of projects on track
🟡 Approximately over 80% of projects on track, but not all
🟢 All projects on track

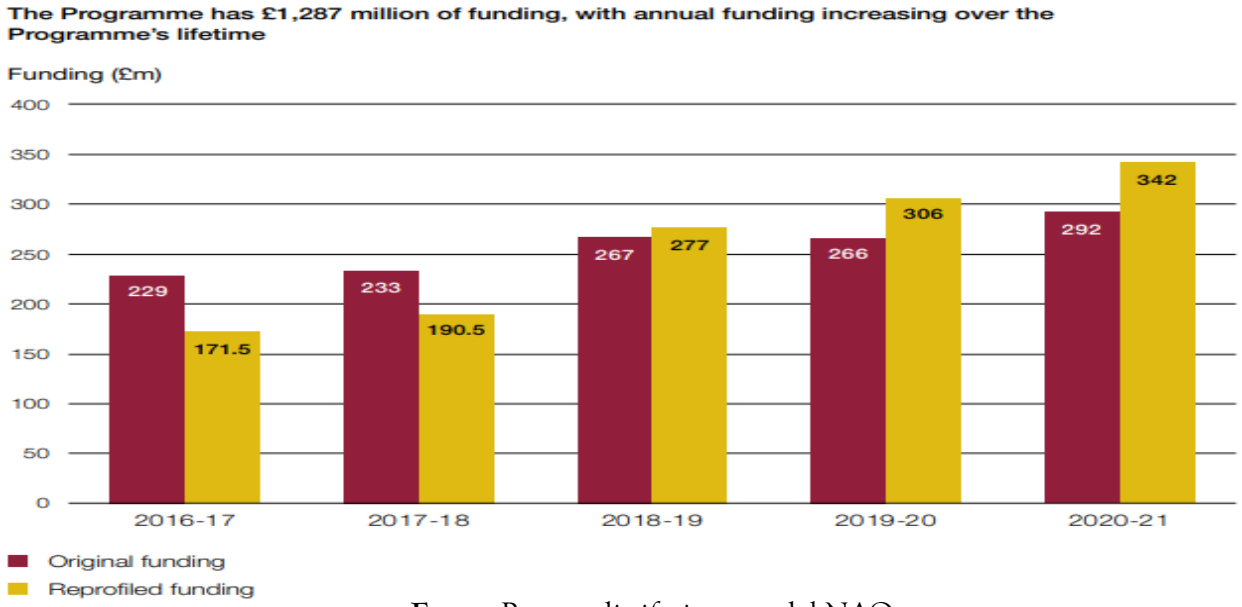
Notes
1 The Strategy's thirteenth objective is not measured as it relates to government's management of the Programme, rather than the effect of the Programme. Part Two provides our view on how well the Programme has been run.
2 NCSC = National Cyber Security Centre; DCMS = Department for Digital, Culture, Media & Sport; FCO = Foreign & Commonwealth Office.

Source: National Audit Office analysis of Cabinet Office data

Fonte: Report di riferimento del NAO

METAVALUTAZIONE
I PUNTI DI FORZA E DEBOLEZZA DELLE CONCLUSIONI

- Si capisce chiaramente come il Governo stia puntando molto su questo programma perché dal primo programma al secondo vi è un aumento da 860 milioni a 1.3 miliardi nell'investimento → **importanza della valutazione del lavoro da parte del NAO.**
  - **Tuttavia l'impiego dei fondi non ha sempre rispettato il criterio di efficienza** → dal report si evince che i fondi stanziati sono si sono rivelati sufficienti, in quanto parzialmente destinati ad altre finalità (come l'antiterrorismo)



Fonte: Report di riferimento del NAO

- **La parte in itinere genera difficoltà nell'avere una valutazione completa e obiettiva della performance** e porta a non poter definire come inefficienti tutti i punti del programma non ancora realizzati, in quanto il Programma non è ancora concluso. Ciò evidenzia che **gli obiettivi del progetto non sono ancora stati completamente raggiunti.**

- Le Raccomandazioni servono come sprone per il governo all'implementazione delle aree di policy ancora incomplete, per evitare di chiudere a marzo 2021 con il progetto in perdita. **Non è chiaro se lo stanziamento dei fondi sia stato canalizzato nell'ottica di raggiungimento dei risultati previsti.**

- **Difficoltà di affermare una valutazione completa sul rapporto tra efficacia delle misure implementate e loro rispettivi costi.**

I. IN SINTESI

IL RAGGIUNGIMENTO DEGLI OBIETTIVI

7

DETER
(deterrenza)

- Il governo ha sviluppato nuovi modi per rilevare e scoraggiare i criminali informatici ✓
- **L'impatto della criminalità informatica sul Regno Unito è stato complessivamente ridotto** ✓
- Date le basse barriere all'ingresso per la criminalità informatica e i bassi livelli di "igiene informatica" è improbabile che si soddisfi l'ambizione della strategia di "ridurre significativamente criminalità informatica nel Regno Unito entro il 2021 ". ✗

DEFEND
(difesa)

- Sono stati compiuti buoni progressi per sviluppare **un'efficace capacità di gestione** per rispondere agli incidenti informatici che colpiscono il Regno Unito e ridurre i danni causati alle organizzazioni e ai cittadini. ✓
- Il governo **non si aspetta di soddisfare l'ambizione fissata** ovvero"tutte le organizzazioni nel Regno Unito devono gestire efficacemente il proprio rischio informatico" entro il 2021.

FONTI

- **NAO – Progress of the 2016-2021 National Cyber Security Programme** https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf
- *Appunti delle lezioni del corso ANALISI E VALUTAZIONE DELLE POLITICHE PUBBLICHE*

II. IN SINTESI
IL RAGGIUNGIMENTO DEGLI OBIETTIVI

7

DEVELOP
(sviluppo)

Ci sono anche alcune prove che il **settore della sicurezza informatica sia in crescita**:

→ 17 università hanno ottenuto l'accreditamento da NCSC come centri accademici di eccellenza nella ricerca sulla sicurezza informatica

→ Il governo sta sviluppando una strategia scientifica e tecnologica sulla sicurezza informatica

Nonostante questi programmi coinvolgano migliaia di potenziali professionisti della sicurezza informatica, questa è una sfida a lungo termine che richiede un supporto costante.
Sono necessari ulteriori progressi

GOVERNANCE

Nel report il discorso sulla **governance è lasciato «in bianco».** Viene però evedenziato che le politiche, le organizzazioni e le strutture del governo sono semplificate per massimizzare la coerenza e l'efficacia nella risposta alla minaccia informatica

FONTI

- **NAO – Progress of the 2016-2021 National Cyber Security Programme** https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf
- *Appunti delle lezioni del corso ANALISI E VALUTAZIONE DELLE POLITICHE PUBBLICHE*

GLI EFFETTI DELLA VALUTAZIONE

A cura di GEMMA BISSANTI (matr. 961896)

GLI EFFETTI DELLA VALUTAZIONE
SUGLI OBIETTIVI DETER- DEFEND

Grazie alla national Cyber Security Strategy:

- Il governo riconosce questa sfida e coinvolge istituzioni, organizzazioni, imprese e cittadini per gestire la propria esposizione al rischio informatico

- Normative e incentivi che migliorano la sicurezza informatica
- Regolamento Generale dei Dati (GDPR)
- Data Protection Act (DPA)
- Direttiva sui sistemi informatici (NIS)

Aumento della consapevolezza del rischio informatico:

- ***EVENTO SCATENANTE*** → l'attacco ramsonware «Wannacry» ha colpito 47 trust dell'NHS e trust di fondazione del Regno Unito
- ***GESTIONE DEL PROBLEMA*** → nominato l'NCSC che collabora con il dipartimento della salute, NHS Digital e l'agenzia nazionale per la criminalità, mentre i ministri hanno attivato il comitato COBR (Cabinet Office Briefing Rooms)

PROGRAMMA «ACTIVE CYBER DEFENSE»:

- *Interventi e servizi gratuiti per la Cyber Protection*

- Il governo attua servizi progettati per incoraggiare i siti di hosting a rimuovere contenuti dannosi, per ridurre i falsi messaggi di posta elettronica provenienti da siti inaffidabili, riducendo così il rischio di Distributed Denial Of Service Attack (DDOS)

GLI EFFETTI DELLA VALUTAZIONE SULL' OBIETTIVO DEVELOP

- Sviluppo del **Cyber Security Body of Knowledge**

- Supporto del governo a imprenditori, start-up e ricerca accademica per rafforzare la sicurezza informatica
  → 17 Università accreditate dall' NSCS

Creati nuovi istituti di ricerca:

- accademici e professionisti acquisiscono consapevolezza della reale emergenza in materia di National Cyber Security

Si delineano le nuove priorità del dipartimento:

- Rendere il governo più sicuro
- Continuare a sostenere e sviluppare il National Cyber Security Center (NCSC)
- Finanziare ulteriormente la ricerca
- Raggiungimento della sicurezza fin dalla progettazione di qualunque dispositivo con possibilità di connessione online →*Internet Of Things Solution* (IoT)
- Revisione delle normative sulla sicurezza informatica

- I dipartimenti hanno coinvolto il FOREIGN & COMMONWEALTH OFFICE (FCO), la COMMISSIONE PER LO SVILUPPO DELL'UNIONE EUROPEA SUI PROGETTI DI SICUREZZA INFORMATICA INTERNAZIONALE e le NAZIONI UNITE

- Il dipartimento fornirà un processo di coordinamento centrale per garantire coerenza e trasparenza sulle singole azioni dei dipartimenti per richiedere i giusti finanziamenti al tesoro HM TREASURY

- Si vuole istituire un nuovo gruppo di lavoro che valuta l'approccio del governo e progetta una rinnovata strategia futura

GLI EFFETTI DELLA VALUTAZIONE

FEEDBACKS

- The Impact of Cyber Security on UK Businesses https://www.youtube.com/watch?v=Dzl6s6TidDg

- L'Università degli studi Oxford e Imperial College London partecipano attivamente al dibattito che ruota attorno alla cyber security
  - → https://www.cybersecurity.ox.ac.uk/
  - → https://www.imperial.ac.uk/media/imperial-college/institute-for-security-science-and-technology/Cyber-report-spreads-lores.pdf

Fonte: OXFORD University

Fonte: imperial College London

GLI EFFETTI DELLA VALUTAZIONE
FEEDBACKS

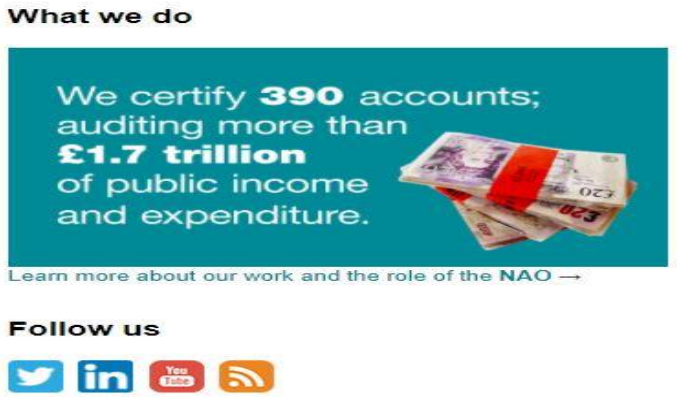
- Inoltre sul web si possono trovare nuove sfide a favore della responsabilizzazione di tutti gli utenti nell'utilizzo dei dispositivi informatici

Fonte: https://www.cybersecuritychallenge.org.uk

- Intanto su twitter si legge l'incombente resa dei conti delle appropriazioni dei dati forniti dagli utenti a facebook ed apple

Fonte: twitter

- Sulla pagina del NAO manca facebook tra i social di pubblicazione mentre sono presenti Twitter, Linkedin, Youtube
  → https://www.nao.org.uk/



Fonte: twitter

IN SINTESI

- Il governo, grazie alla National Cyber Security Strategy ha intrapreso delle azioni concrete rispetto alla sicurezza informatica
- Emerge la volontà di istituire un nuovo gruppo di lavoro che valuta l'approccio del governo e progetta una rinnovata strategia futura
- Si sta sviluppando una campagna di sensibilizzazione attiva di tutti gli utenti che utilizzano la rete Internet ed i vari dispositivi informatici

FONTI

- **NAO – Progress of the 2016-2021 National Cyber Security Programme** https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf
- Facebook, Twitter
- https://www.cybersecurity.ox.ac.uk
- https://www.imperial.ac.uk/media/imperial-college/institute-for-security-science-and-technology

GRAZIE PER L'ATTENZIONE!

NATIONAL CYBER SECURITY STRATEGY 2016-2021

ASSERO – BARAZZETTA – BIANCHI - BISSANTI – CAVANNA – COLOMBO – MIDURI - SALA