



BAN CƠ YẾU CHÍNH PHỦ

TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ GIÁM SÁT AN NINH MẠNG

HOẠT ĐỘNG GS ATTT VÀ GIẢI PHÁP ĐẢM BẢO ATTT CỦA BAN CƠ YẾU CHÍNH PHỦ CHO MẠNG CNTT CỦA CÁC CƠ QUAN NHÀ NƯỚC

Người trình bày: PGS.TS Trần Đức Sự



NỘI DUNG

1 Tình hình ATTT hiện nay

2 Giải pháp đảm bảo ATTT của Ban Cơ yếu Chính phủ

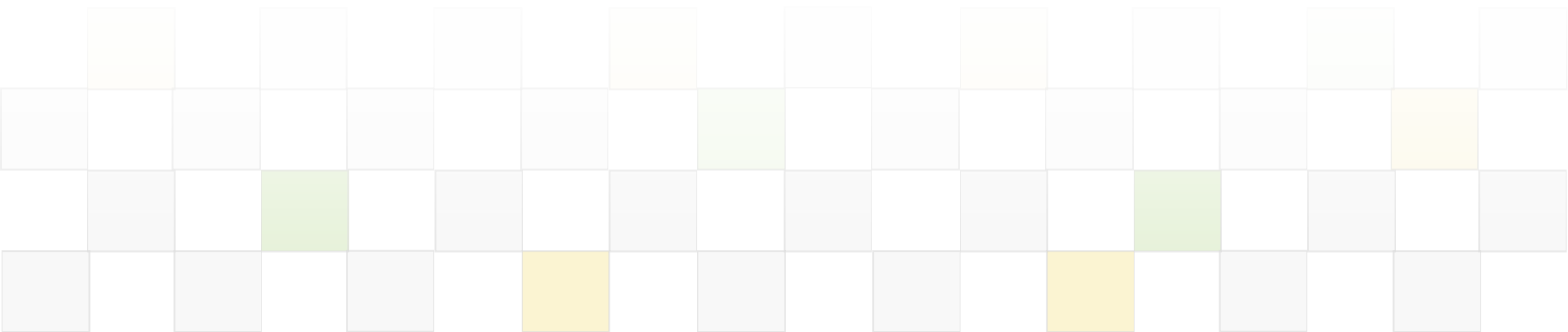
3 Hoạt động GS ATTT của Ban Cơ yếu Chính phủ

4 Khuyến nghị, đề xuất

5 Kết luận



TÌNH HÌNH AN TOÀN THÔNG TIN HIỆN NAY





Tình hình ATTT hiện nay

❖ Thế giới:

- ✓ Các cuộc tấn công mạng diễn ra liên tục, hình thức tinh vi và quy mô thì cũng đa dạng gây thiệt hại khoảng 400 tỷ USD mỗi năm (Theo Fireeye)





Tình hình ATTT hiện nay

- ✓ Các nhóm tội phạm mạng gia tăng với sự hỗ trợ của các tổ chức kinh tế, chính trị (Nhóm APT1, APT30 được nghi là thuộc Trung quốc, Nhóm ATP28 – Nga, vv..)





Tình hình ATTT hiện nay

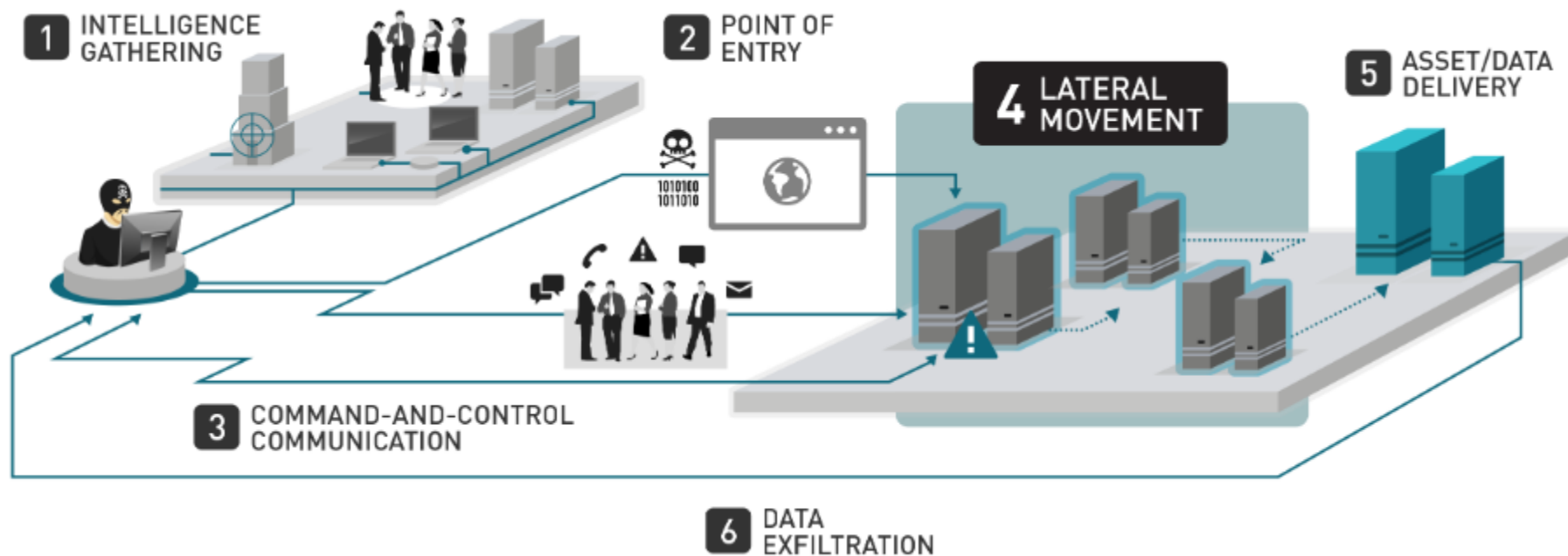
- ✓ Các chính phủ chạy đua thành lập các lực lượng quân đội mạng, sẵn sàng cho chiến tranh mạng (Cybercom của Mỹ; 61398 – Trung Quốc; lực lượng chiến tranh mạng của Nga; Lực lượng An ninh mạng – Nato)



Tình hình ATTT hiện nay

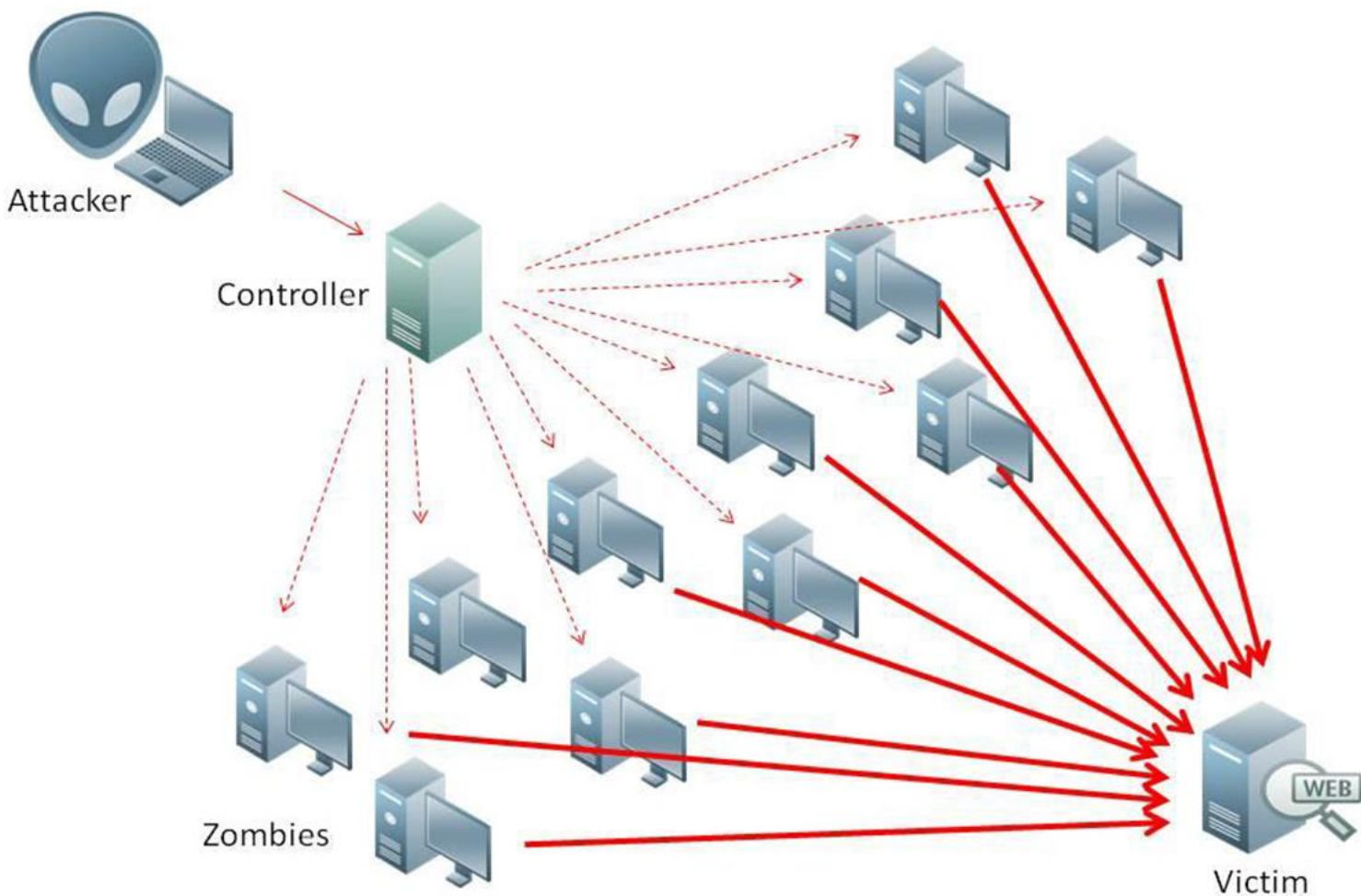
Các dạng tấn công phổ biến được sử dụng:

✓ Tấn công có chủ đích:



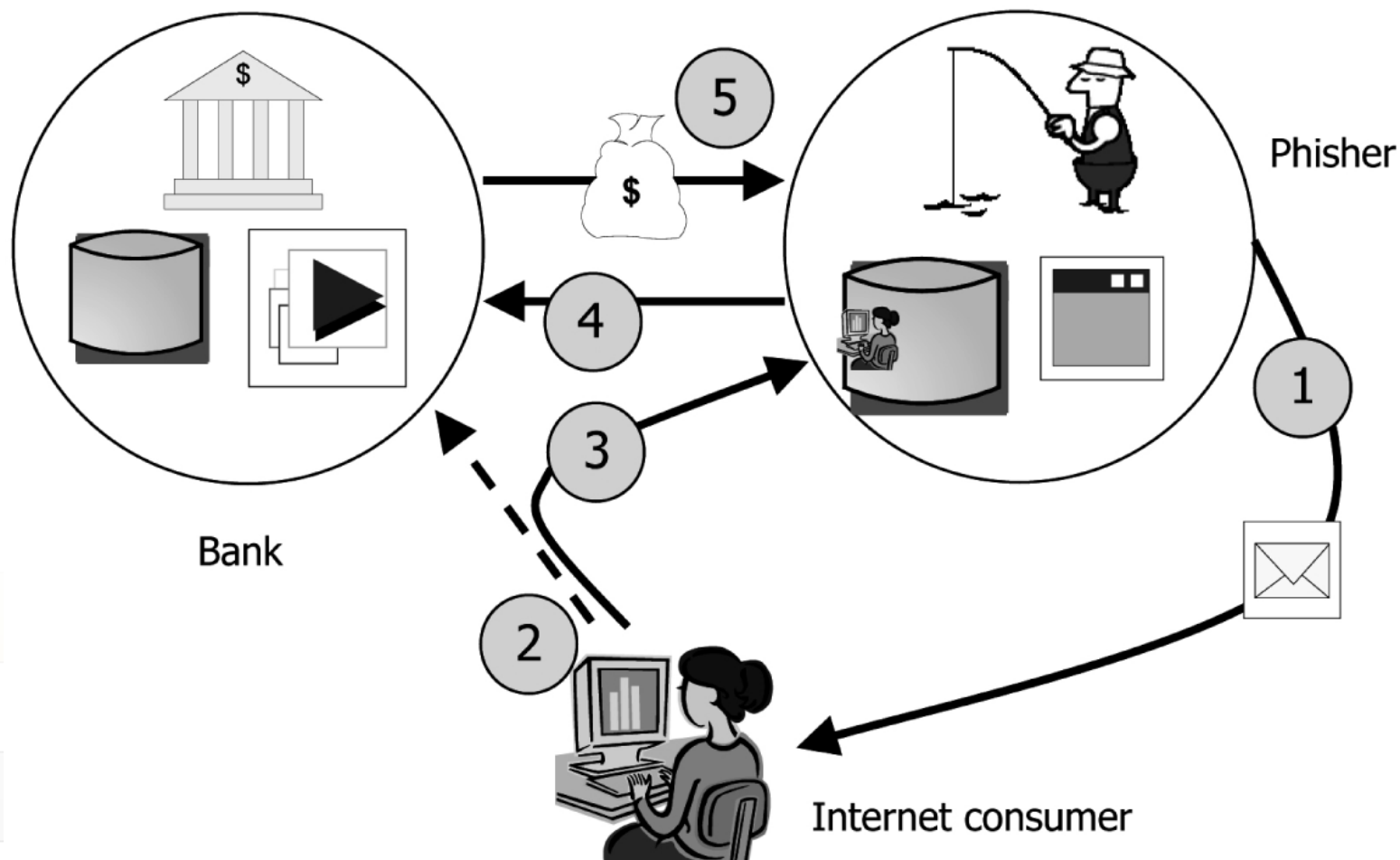
Tình hình ATTT hiện nay

✓ Tấn công từ chối dịch vụ:



Tình hình ATTT hiện nay

✓ Tấn công lừa đảo người dùng:





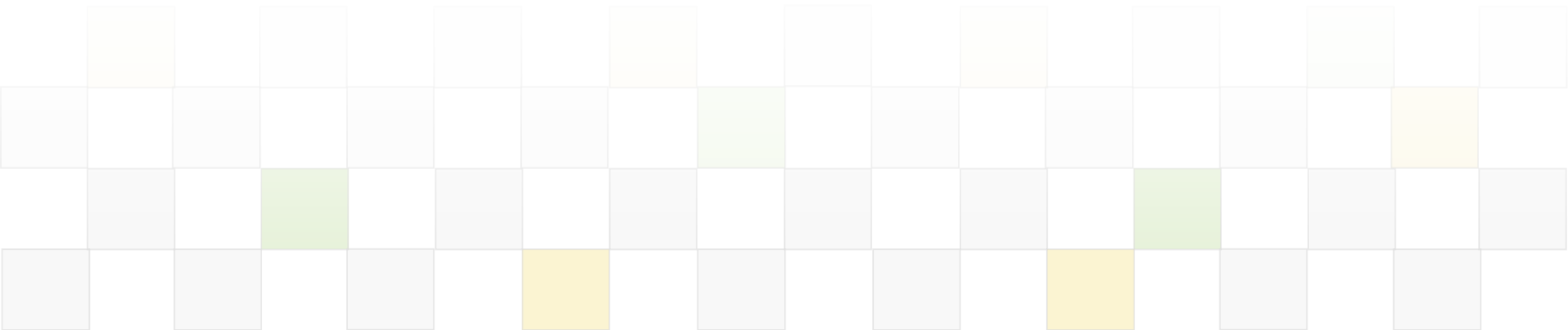
Tình hình ATTT hiện nay

❖ Trong nước:

- ✓ Chịu sự tác động từ hình an ninh, an toàn thông tin của thế giới
- ✓ Người dùng bị tấn công mạng đứng thứ 6/10 các quốc gia bị tấn công nhiều nhất (Theo Kaspersky 2014)
- ✓ 68% doanh nghiệp tại Việt Nam cho biết từng bị rò rỉ thông tin quan trọng ra bên ngoài tổ chức. (Theo Symatec).
- ✓ Số lượng các cuộc tấn công vào các mạng của các cơ quan chính phủ, nhà nước liên tục tăng với các hình thức đa dạng và kỹ thuật tinh vi như tấn công APT, tấn công khai thác lỗ hổng; tấn công từ chối dịch vụ. (Theo theo thống kê dữ liệu giám sát của Trung tâm CNTT&GSANM – Ban cơ yếu Chính Phủ)



Giải pháp đảm bảo ATTT của Ban Cơ yếu Chính phủ





2. Giải pháp đảm bảo ATTT của Ban Cơ yếu Chính phủ

- ❖ Ban Cơ yếu Chính phủ là cơ quan mật mã quốc gia, quản lý chuyên ngành về Cơ yếu, sử dụng mật mã để thực hiện nhiệm vụ bảo mật thông tin phục vụ sự lãnh đạo, chỉ đạo của Đảng và Nhà nước.
- ❖ Thời gian qua, Ban Cơ yếu Chính phủ đã chủ động nghiên cứu, phát triển đồng bộ các giải pháp và phối hợp chặt chẽ với các Bộ ngành trung ương và các tỉnh, thành địa phương để đảm bảo ATTT cho các cơ quan này.



2. Giải pháp đảm bảo ATTT của Ban Cơ yếu Chính phủ

Ban Cơ yếu Chính phủ đã triển khai một số nhiệm vụ trọng tâm bao gồm:

(1)

Triển khai các hệ thống bảo vệ thông tin bí mật nhà nước dùng mật mã.

(2)

Triển khai hệ thống chứng thực điện tử và chữ ký số (CA) phục vụ các cơ quan thuộc hệ thống chính trị

(3)

Triển khai giám sát an toàn thông tin (GS ATTT) trên mạng CNTT trọng yếu của Đảng và Chính phủ.

(4)

Quản lý mật mã phục vụ hoạt động kinh tế xã hội



2.7 Giải pháp đảm bảo ATTT của Ban Cơ yếu Chính phủ

Một số đặc điểm chung của mạng CNTT trong cơ quan Nhà nước:

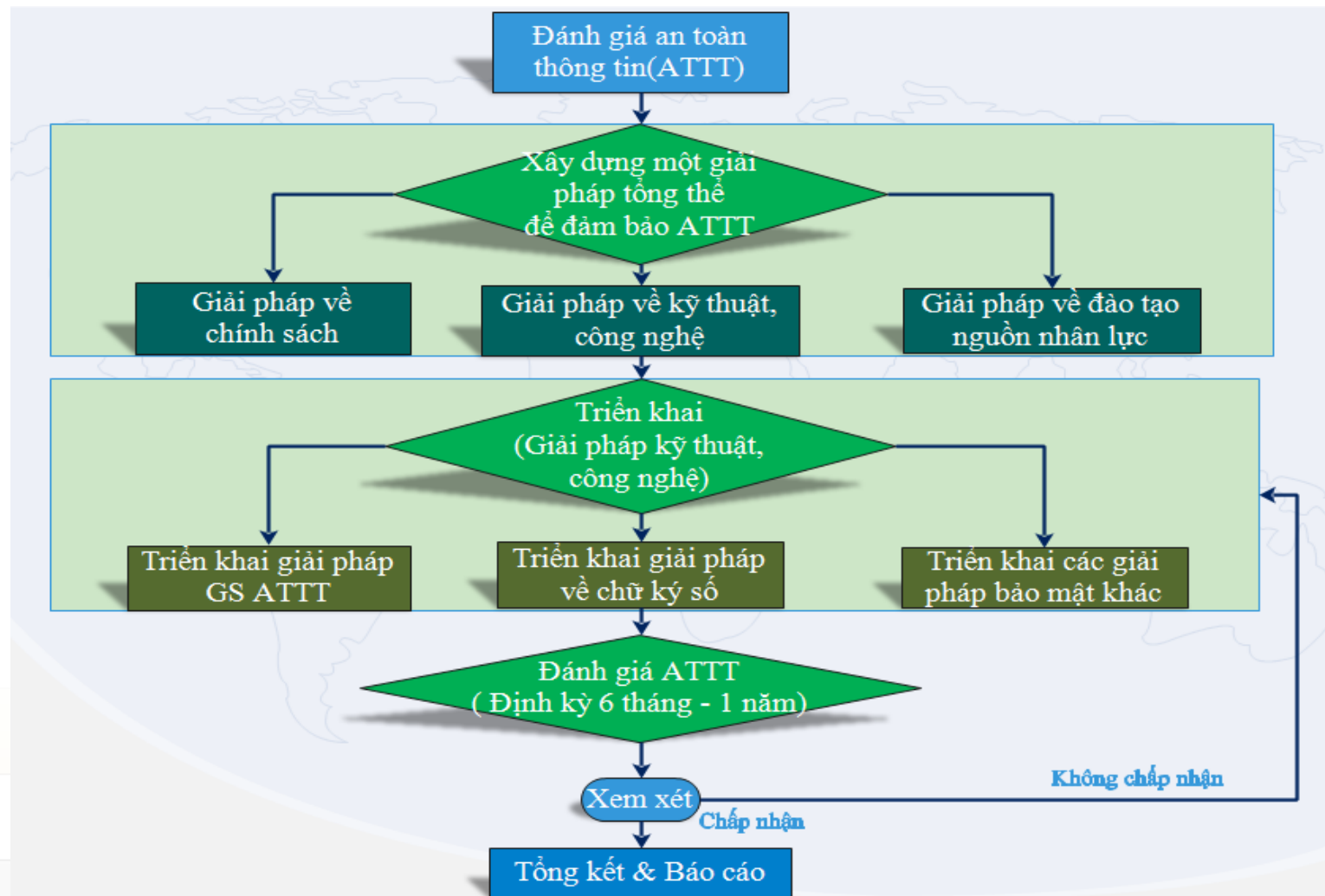
- Triển khai các giải pháp đảm bảo ATTT, bảo mật còn yếu và chưa đồng bộ.
- Đội ngũ chuyên trách đảm bảo ATTT còn thiếu và chưa được đào tạo chuyên sâu. Nhận thức của người dùng về ATTT còn chưa cao dễ dẫn đến nguy cơ lộ lọt, mất ATTT.
- Quy chế, chính sách về ATTT còn ở mức độ khác nhau, chưa thực hiện và giám sát một cách toàn diện, triệt để.

Nghị định 72 năm 2013 của Chính phủ đã định nghĩa:

“ATTT là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin”



2/ Giải pháp đảm bảo ATTT của Ban Cơ yếu Chính phủ

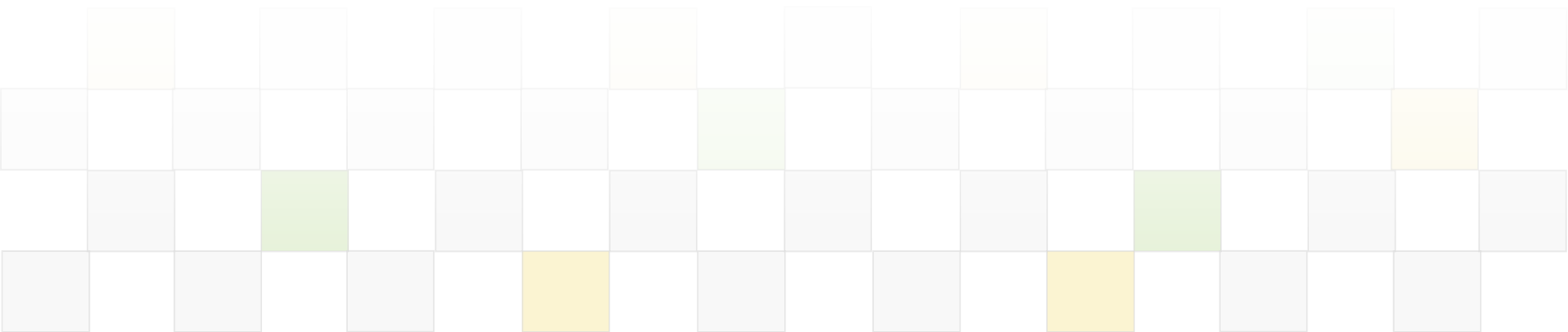


Quy trình triển khai giải pháp đảm bảo ATTT của Ban Cơ yếu Chính phủ



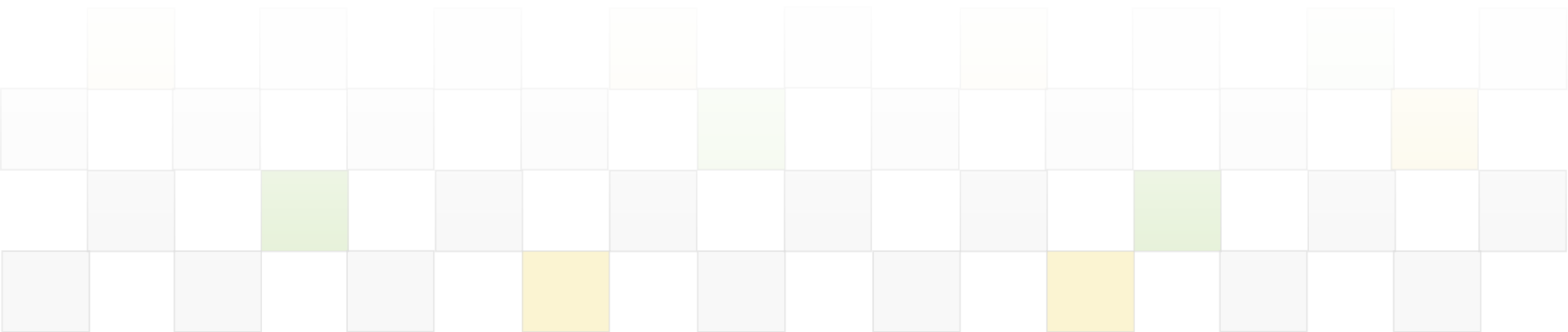
2. Giải pháp đảm bảo ATTT của Ban Cơ yếu Chính phủ

- ❖ Sản phẩm, giải pháp của Ban Cơ yếu Chính phủ:
 - Sản phẩm, giải pháp liên quan đến bảo mật
 - Sản phẩm, giải pháp liên quan đến chứng thực chữ ký số
 - Sản phẩm, giải pháp liên quan đến GS ATTT
- ❖ Sản phẩm, giải pháp của Ngành Cơ yếu đã bao trùm và đáp ứng được yêu cầu đảm bảo ATTT.





Hoạt động GS ATTT của Ban Cơ yếu Chính phủ

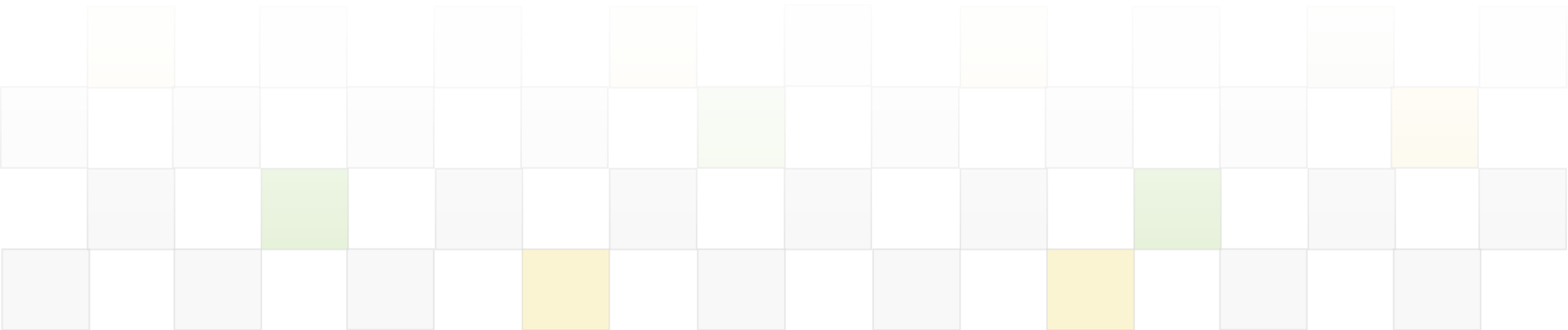




3. Hoạt động GS ATTT của Ban Cơ yếu Chính phủ

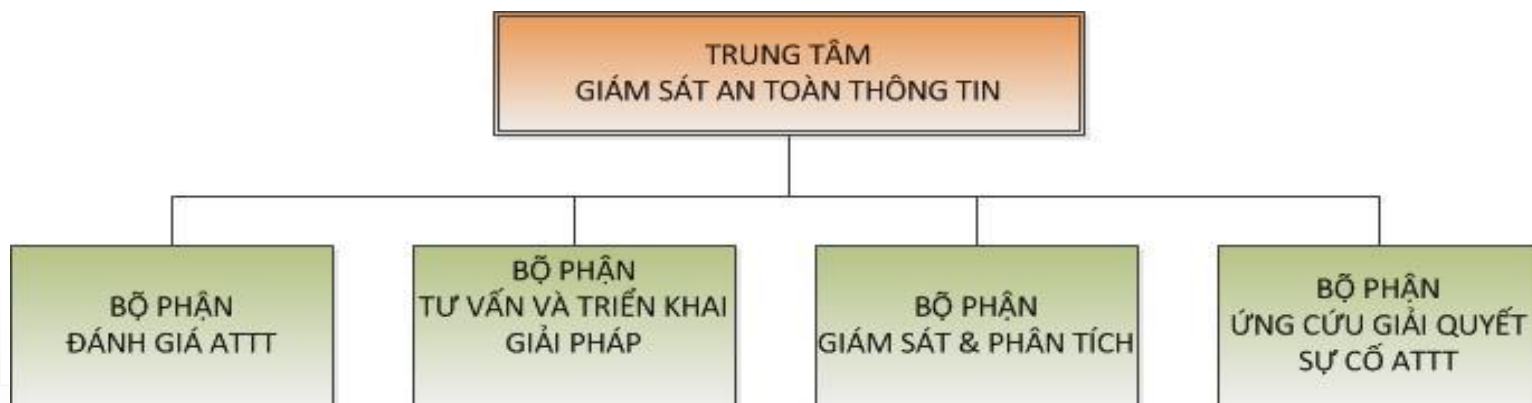
Nhiệm vụ GS ATTT được Đảng, Chính phủ giao cho Ban Cơ yếu Chính phủ thông qua:

- Quyết định 66 của Thủ tướng năm 2006 về phê duyệt quy hoạch tổng thể phát triển Ngành Cơ yếu Việt Nam đến năm 2010 và định hướng đến năm 2020.
- Luật Cơ yếu
- Luật tổ chức chính phủ
- Luật an toàn thông tin mạng



3. Hoạt động GS ATTT của Ban Cơ yếu Chính phủ

- Từ năm 2006, Ban Cơ yếu Chính phủ đã xây dựng Trung tâm GS ATTT đặt tại Trung tâm CNTT và GSANM.
- Đến nay, Hệ thống GS ATTT đã và đang được triển khai cho gần 20 mạng CNTT trọng yếu của các cơ quan Trung ương, Bộ ngành và Tỉnh thành (như Bộ Ngoại giao, Bộ Tư pháp, TP Hồ Chí Minh ...).



Mô hình tác nghiệp GS ATTT

3.1 Giải pháp triển khai GS ATTT của Ban Cơ yếu chính phủ



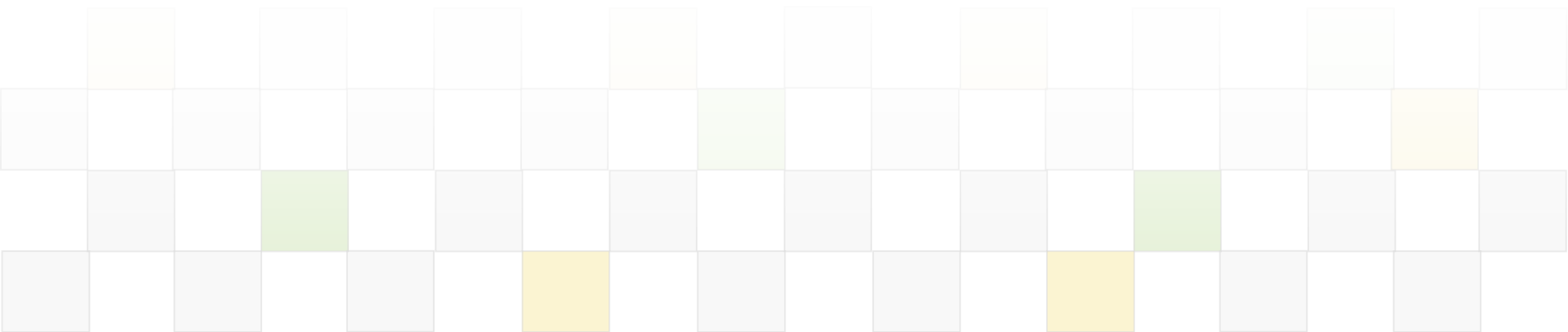
Mô hình giám sát ATTT của Ban Cơ yếu Chính phủ



3. Hoạt động GS ATTT của Ban Cơ yếu Chính phủ

Lợi ích khi triển khai Hệ thống GS ATTT:

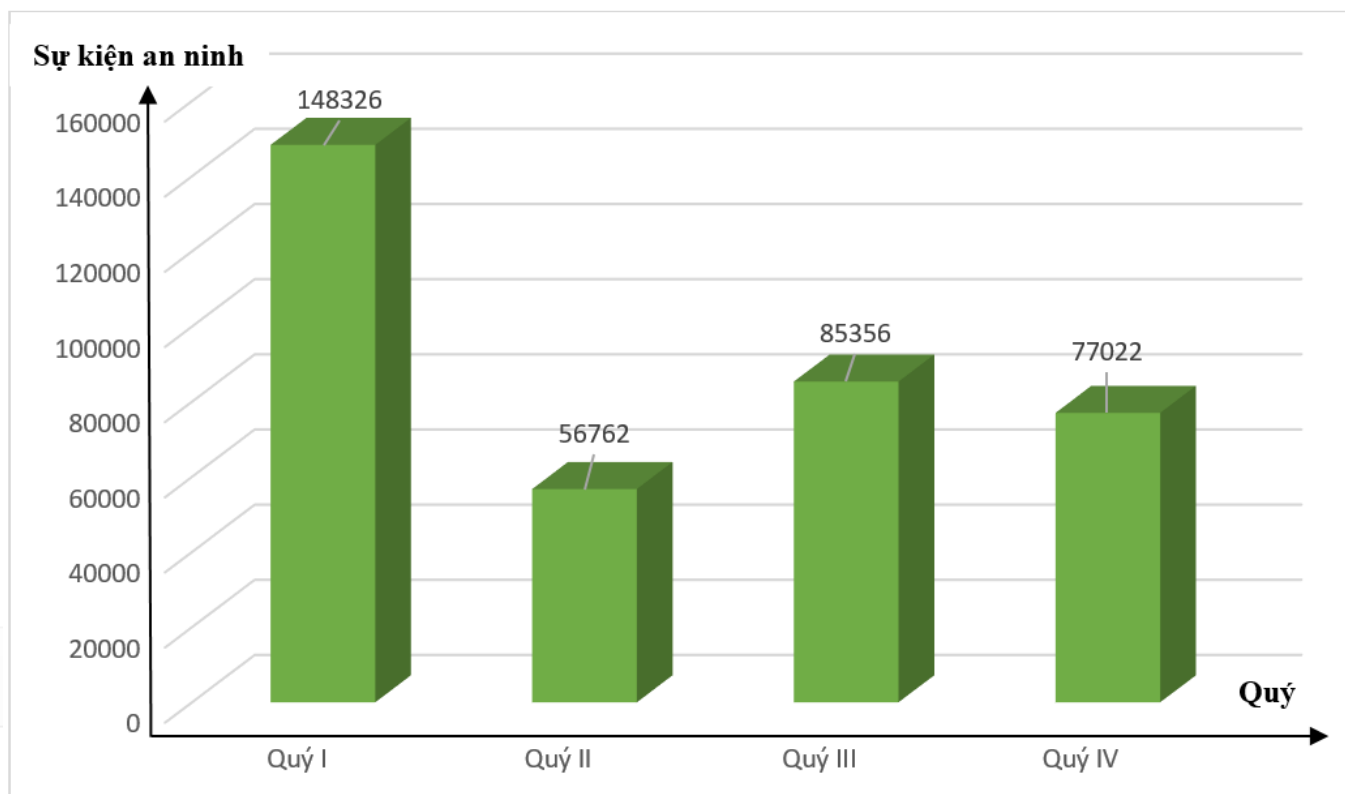
- Phát hiện các tấn công mạng.
- Phát hiện các điểm yếu, lỗ hổng bảo mật của các thiết bị, ứng dụng và dịch vụ trong hệ thống.
- Phát hiện sớm để ngăn chặn các tấn công có chủ đích APT.
- Giám sát việc tuân thủ chính sách an ninh trong hệ thống.
- Cung cấp bằng chứng số phục vụ công tác điều tra sau sự cố.





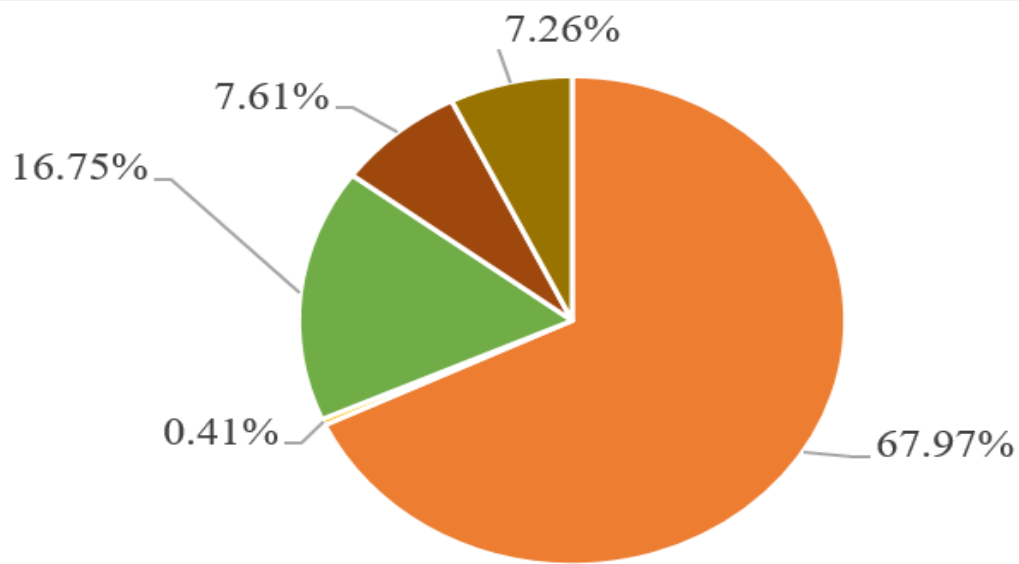
3. Hoạt động GS ATTT của Ban Cơ yếu Chính phủ

- Dưới đây là số liệu về tấn công mạng trên các mạng đại diện cho các khu vực Trung ương, Bộ ngành và Tỉnh thành mà Hệ thống GS ATTT ghi nhận được trong năm 2015:



Số lượng cảnh báo tấn công theo từng Quý năm 2015

3. Hoạt động GS ATTT của Ban Cơ yếu Chính phủ



- Tấn công liên quan đến dò quét cổng, lỗ hổng
- Tấn công liên quan đến dò quét mật khẩu, xác thực
- Hiện tượng bất thường
- Exploit, malware, botnet
- Vi phạm chính sách

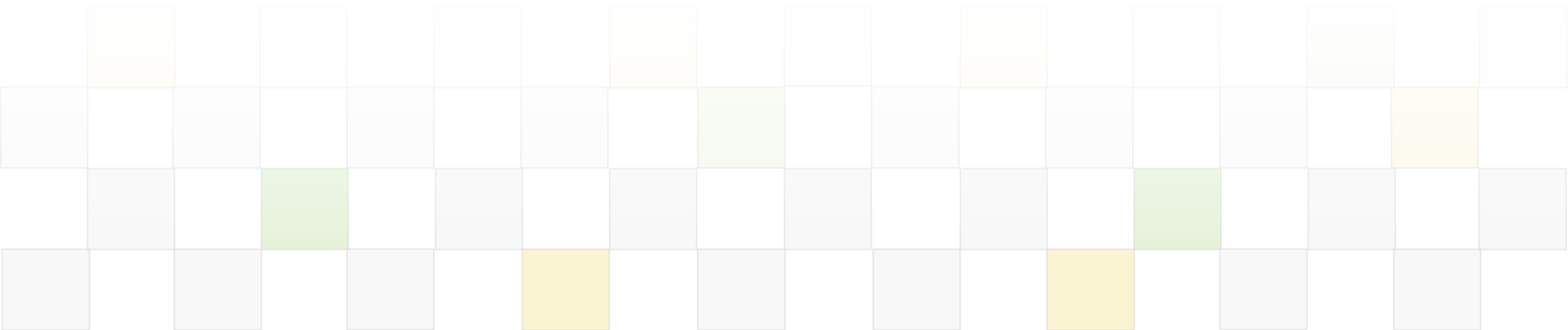
Các loại cảnh báo tấn công mạng năm 2015



3. Hoạt động GS ATTT của Ban Cơ yếu Chính phủ

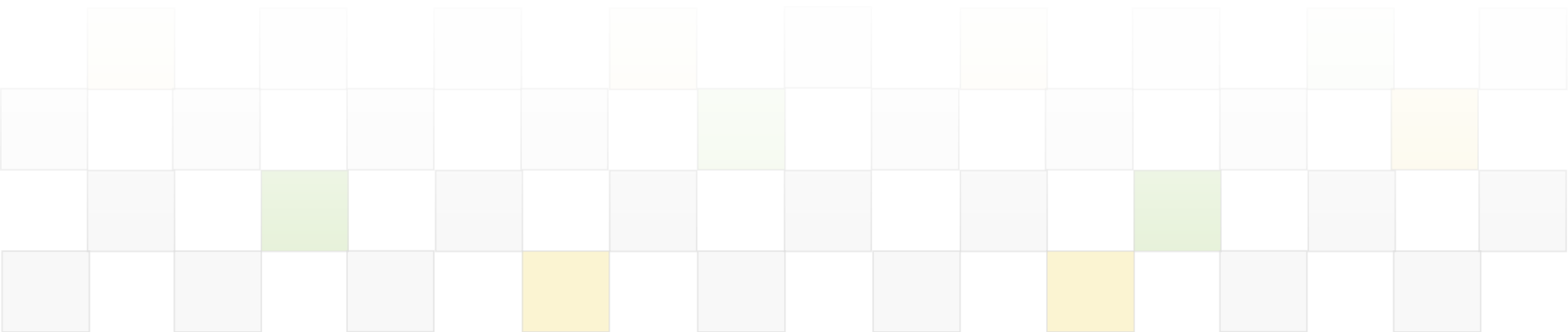
Trong quá trình triển khai, Trung tâm CNTT & GSANM - Ban Cơ yếu Chính phủ đã phối hợp chặt chẽ với các cơ quan phụ trách các mạng được giám sát để:

- Cung cấp kịp thời các cảnh báo về tấn công, điểm yếu lỗ hổng bảo mật.
- Cung cấp các giải pháp để ngăn chặn kịp thời các tấn công này không để xảy ra các sự cố nghiêm trọng.





Khuyến nghị, đề xuất





4. Khuyến nghị, đề xuất

Để tăng cường ATTT cần triển khai đồng bộ 03 giải pháp liên quan đến: chính sách, kỹ thuật công nghệ và nguồn nhân lực:

- ***Chính sách:***

Thời gian qua Nhà nước rất quan tâm đến ATTT, thể hiện qua:

- Chỉ thị 15/CT -TTG ngày 17/06/2014 của Thủ tướng: tăng cường bảo đảm an ninh an toàn thông tin mạng trong tình hình mới;
- Nghị định số 09/2014/NĐ-CP ngày 27/1/2014 của Chính phủ về chức năng, nhiệm vụ, quyền hạn của Ban Cơ yếu Chính phủ;
- QĐ 260 năm 2014 của Ban Bí thư về đẩy mạnh ứng dụng phát triển CNTT đáp ứng nhu cầu phát triển bền vững;
- Chỉ thị số 28-CT/TW, ngày 16-9-2013 của Ban Bí thư T.Ư' Đảng (khóa XI) về tăng cường công tác bảo đảm an toàn thông tin mạng;

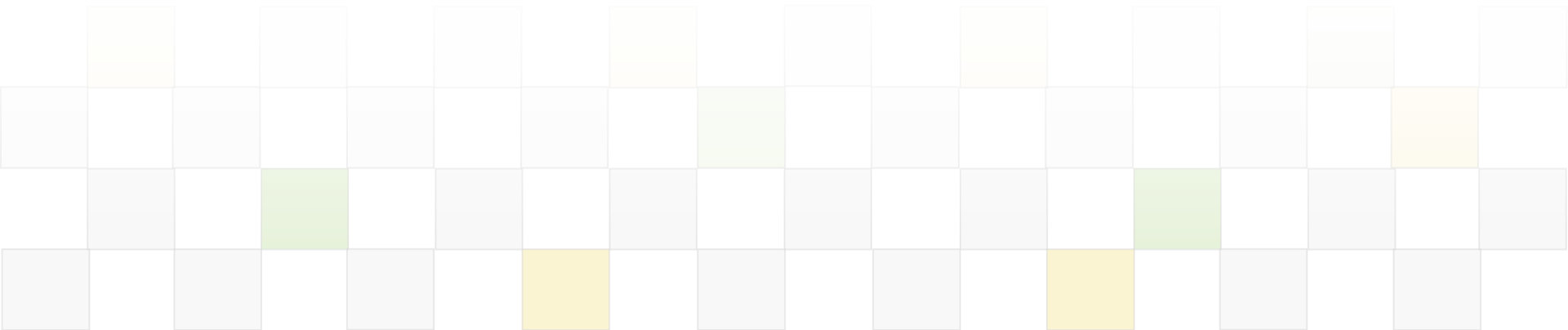


4. Khuyến nghị, đề xuất

- Luật Cơ yếu năm 2011;
- Chỉ thị 897/CT -TTG ngày 10/06/2011 của Thủ tướng: tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số.
- Quy chế phối hợp giữa 03 bộ: Quốc phòng, Công an và TT & TT.
- Quyết định 26 của Thủ tướng về “Chương trình hành động của Chính phủ về Nghị quyết 36 của Bộ Chính trị”.

Tuy nhiên, trong thời gian tới cần:

- Hoàn thiện hệ thống pháp luật về ATTT (Luật ATTT).
- Xây dựng và thực thi triệt để quy chế đảm bảo ATTT tại cơ quan đơn vị.





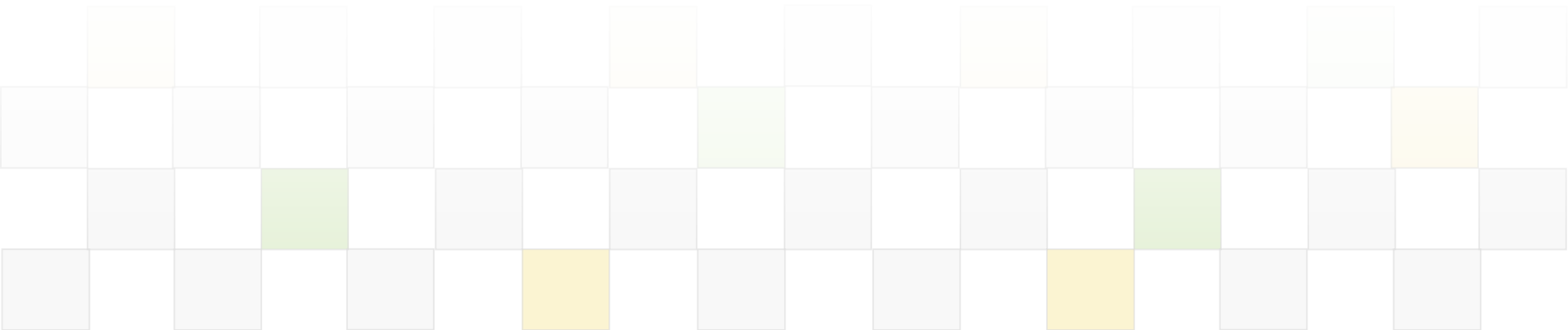
4. Khuyến nghị, đề xuất

- **Nguồn nhân lực:**

Đã được Nhà nước quan tâm thông qua:

- Quyết định số 99/QĐ-TTg ngày 14/01/2014 về đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020.

Trong thời gian tới cần tiếp tục:

- Tăng cường đầu tư, nâng cao tiềm lực cho lực lượng chuyên trách đảm bảo an ninh, an toàn mạng thông tin quốc gia.
 - Nâng cao nhận thức, đề cao tinh thần trách nhiệm trong việc đảm bảo ATTT của đội ngũ lãnh đạo, cán bộ kỹ thuật và người dùng.
- 

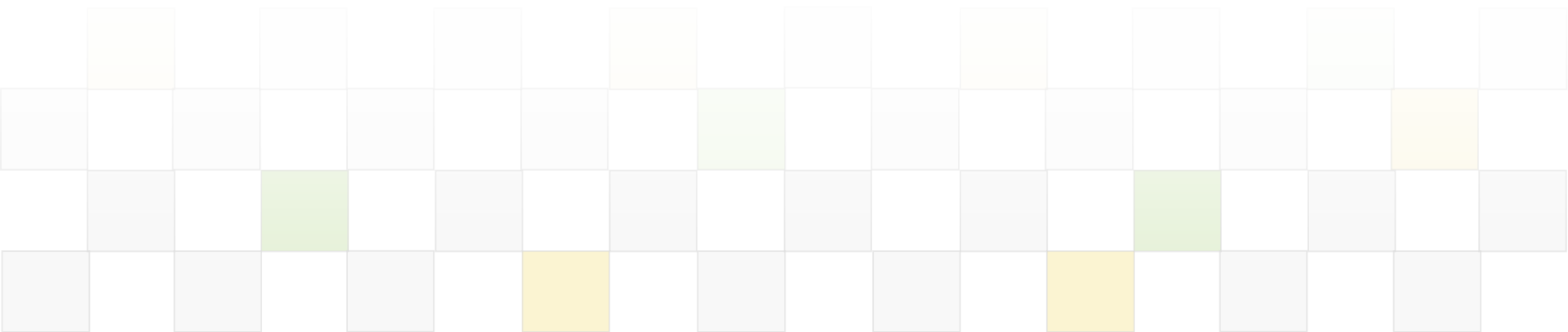


4. Khuyến nghị, đề xuất

- ***Kỹ thuật, công nghệ:***
 - Cần triển khai GS ATTT và các giải pháp đồng bộ khác để đảm bảo cả ba tính toàn vẹn, bí mật và sẵn sàng.
 - Ưu tiên nghiên cứu, sản xuất các giải pháp, công nghệ trong nước phục vụ cho việc đảm bảo ATTT.



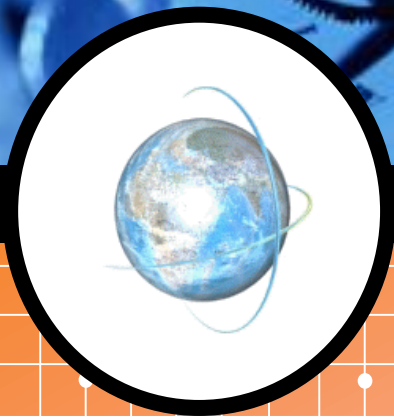
KẾT LUẬN





5. KẾT LUẬN

- Trong bối cảnh các nguy cơ và hiểm họa gây mất an toàn thông tin ngày càng nhiều và mức độ kỹ thuật sử dụng ngày càng tinh vi. Việc tăng cường triển khai đồng bộ, tổng thể các giải pháp đảm bảo ATTT trong đó có GS ATTT cho các cơ quan Nhà nước là việc hết sức cần thiết và cấp bách.
 - Ban Cơ yếu Chính phủ đã chủ động nghiên cứu đưa ra nhiều giải pháp để đảm bảo ATTT và cũng đã triển khai có hiệu quả các giải pháp này ở nhiều cơ quan.
 - Trong thời gian tới, Ban Cơ yếu Chính phủ sẽ tiếp tục phối hợp chặt chẽ với các Bộ ngành, các tỉnh, thành địa phương để tiếp tục triển khai Hệ thống GS ATTT cũng như các giải pháp đảm bảo ATTT khác.
- 



Thank You !