أمن الاتصالات

بقلم القائد/ سيف العدل

هو مجموعة الإجـراءات الـتي تكفـل منـع العـدو مـن الحصول على معلومات عن طريق الاتصالات وتقـوم أيضـاً بمنعه من التدخل الفني أو التكتيكي على شبكة الاتصــالات - التـدخل الفنـي؛ عـن طريـق الـدخول فـي خـط الهـاتف، التدخل التكتيكي؛ عن طريق فك الشفرة –

أولاً: الأخطار التي تواجه الاتصالات:

1) التصـنت عـن طريـق العملاء المجهزيـن بـأجهزة خاصة للتجسس على الهاتف أو من خلال أمن السنترال.
2) القبض أو التفتيش.
3) الحوادث.

ثانياً: وسائل الاتصال المستخدمة:

1) السعاة:

السعاة مفردهـا سـاعي وهـو الشـخص الموكـل إليـه تحقيق الاتصال بين الطرفين باليد بينما يتم التأكد مـن نقـل المعلومة أو الوثيقة عن طريق السلكي أو الإيصال.

أ) مزايا السعاة:

1) مؤمنة جداً.
2) التأكد من وصول المعلومة.
3) غير قابلة للكشف إلا في ظروف ضيقة جداً.

ب) عيوب السعاة:

1) تفتقد إلى السرعة.
2) الساعي عرضة للتجنيد من المعادين.
3) عرضة للحوادث أثناء النقل.

ج) تأمين السعاة:

1) اختيار الساعي على قدر من الخلق والاستقامة.
2) تحديد وتأمين المحاور التي يسلكها الساعي.

3) تدريب العاملين على كيفية إعدام الوثائق عند الخطر.
4) عدم الالتزام بتوقيت زماني أو مكاني معين في نقل الرسائل.
5) تغيير السعاة باستمرار من آن لآخر.

2) البريد العادي:

وسيلة نقل ممتازة لكنها عرضة للسرقة والرقابة وغير سريعة ويمنع استخدامها في نقل الوثائق والمعلومات الهامة جداً.

3) الحقيبة الدبلوماسية:

وسيلة مؤمنة بسبب الحصانة الدبلوماسية.

4) الاتصال السلكي - هاتف/ فاكس/ تلكس - والهواتف النقالة:

اتصالات سريعة جداً وكفاءتها عالية واستخداماتها واسعة ولكنها عرضة للرصد والتصنت ومكلفة جداً في تأمينها.

كيف يتم الرد على التليفون؟

من السهل جداً على جهاز الاستخبارات الحصول على معلومات بطريقة بسيطة منك كالآتي:

الاتصال برقم هاتفك ومحاولة الحصول على معلومات كالآتي:

أ) السؤال المغلوط: يقول لك: هل هذا أبو حسين؟ يكون الرد: لا يا أخي، أبو حسين ليس موجود. فيقول لك: متى يأتي؟ هل هو مسافر؟

وهكذا قد يستطيع الحصول منك على معلومات من خلال طريقة الحديث أو غيرها.

ب) يقول لك: من معي؟ فيجيبه الأخ: معك أبو أحمد، فيحاول أن يسألك بعض الأسئلة التي يجمع من وراءها معلومات.

انتبه...

- لا تعط أي معلومات من خلال التليفون.
- لا تـذكر اسـمك أو معلومـات عـن أي أخ آخـر، أو تعطي معلومات عن تحركات، أو وجود شـخصٍ مـا أو عـدم وجوده ، لا تعط أي بيانات.

الهواتف الثابتة والنقالة خطيرة جداً:

تعتبر الهواتف سواءً الثابت منها أو النقال مـن اخطـر الأمور، وأكثر المعلومات التي يتحصل عليها العدو هـي مـن الهاتف، ومن أكثر المداخل التي يؤتى المجاهدون من قبلها هي الهواتف، فكم من أخ تساهل في أمر الاتصال وكم مـن أخ تساهل في أمر كتابة الأرقـام ووضـعها فـي نوتـة خاصـة فإذا سقطت سقط معها الكـثير مـن الشـباب وأيضـاً، لعـل المتابع لحال الإخوة في فلسطين يرى كيف اسـتغل اليهـود الهواتف النقالة فـي تصـفية واغتيـال الكـثير مـن القيـادات والكـوادر، فعلـى الشـباب المجاهـد تفـويت الفرصـة علـى الأعداء وعدم إكسابهم أي أمر والله وحده الحافظ من قبل ومن بعد.

بعض الأمثلة عن أخطاء حدثت في عمليات ضد الحكومات بسبب التساهل في تأمين الاتصالات:

المثال الأول: في عملية اغتيال حدثت في مصـر - اشتبهت الحكومة المصرية في أن مدبري الحـادث ينتمـون إلى جماعة إسلامية في بيشاور - ولم تتمكن الحكومة مـن ضـبط أحـد فـي الحـادث. فقـامت الحكومـة بوضـع رقابـة مشددة على تليفونات اعتـادت الجماعـة الاتصـال بهـا فـي مصـر، وبعـد 3 أيـام التقطـت مكالمـة مـن بيشـاور وهـذه المكالمة تحدد موعد للقاء فـي القـاهرة وقـامت الحكومـة بعمل كمين واعتقلت المسئولين عن الحادث.

المثـال الثـاني: عمليـة اغتيـال "شـهبور بختيـار" رئيس وزراء إيران السابق في فرنسا في عام 1992م :

كان "شهبور بختيار" يعيش في فيلا في فرنسا وعليه حراسة مشـددة مـن البـوليس الفرنسـي لمـدة 24 سـاعة متواصـلة. زاره أحـد العـاملين المقربيـن منـه والمعـروف لطاقم الحراسة، وعندما وصل إلى فلتـه وكـان معـه اثنيـن

آخرين إيرانيين سمح لهم البوليس بالدخول بعد تفتيشهم وتركوا جوازات سفرهم بالباب. دخلوا فحياهم "شهبور" وجلسوا ودخل سكرتير "شهبور" لإعداد الشاي في المطبخ فقفز هؤلاء على "شهبور" وقتلوه ثم قاموا بقتل السكرتير ومكثوا ساعة واحدة في الشقة ثم غادروا الفيلا وأخذوا جوازات سفرهم ورحلوا في السيارة.

ذهب معاون "شهبور" في طريق، والاثنان الآخران استقلوا القطار وتوجهوا إلى الحدود الفرنسية السويسرية لعبورها ولكن جمرك الحدود السويسري شك في تأشيرة الدخول إلى سويسرا ورفض السماح لهم بالدخول.

تحركوا إلى نقطة حدود أخرى ونجح أحدهما في الدخول إلى سويسرا ولم ينجح الآخر وبقي في داخل فرنسا هائماً على وجهه لمدة 5 أيام.

اكتشفت جثة "شهبور" بعد 48 ساعة من مقتله وقام البوليس بنشر صور المتهمين الثلاثة، وتم اعتقال الشخص الذي لم ينجح في الخروج من فرنسا، ولكنه أنكر صلته بالقتل وقال بأنه كان متواجداً فقط.

اشتبهت السلطات الفرنسية في أن الحكومة الإيرانية لها يد في هذه الجريمة فأرادت أن تثبت ذلك وقامت بعمل الآتي:

أ) قامت الحكومة بفحص جميع الكبائن العامة الموجودة على خط السير الذي تحرك فيه الرجلان في اتجاه الحدود السويسرية فأحصت أكثر من 20 ألف مكالمة في فترة الخمسة أيام قبل أن يتم القبض على هذا الرجل الذي لم يستطع الخروج.

ب) بعد الفحص الدقيق وجدت الحكومة تطابق في عدة مكالمات إلى شقتين في استنبول بتركيا وبالتالي تحددت هاتين الشقتين على أنهما مركز قيادة العملية.

ج) بعد ذلك طلبت الحكومة الفرنسية من الحكومة التركية المساعدة فقامت الحكومة التركية بفحص التليفونات الصادرة من هاتين الشقتين وهما مملوكتين لمواطن إيراني وأعطت البيانات إلى الاستخبارات الفرنسية وكانت المكالمات صادرة إلى:

- وزارة الخارجية الإيرانية.
- مكتب استخبارات إيراني مسئول عن العمليات الخاصة.
- شقة في فرنسا؛ قامت السلطات الفرنسية باستجواب صاحبتها فاعترفت بأنها تعمل عميلة مع الاستخبارات الإيرانية، تم فحص المكالمات الصادرة من شقة فرنسا وكانت صادرة إلى تركيا وإيران.

الخلاصة انه بمعرفة أرقام التليفونات تم الربط بين المنفذين والحكومة الإيرانية

كيف تسيطر الحكومة على التليفون؟

التليفونات تعمل بنظام الكمبيوتر، أي أن هناك كمبيوتر مركزي يستطيع الدخول على أي تليفون أو إعطاء بيانات عن أي تليفون في الدولة مثل: أرقام التليفونات التي قام هذا التليفون بالاتصال بها لأنها مسجلة في الكمبيوتر واسم صاحب التليفون وبياناته وهكذا...

وهذا تراه عندما تستلم فاتورة التليفون تكون كالآتي: هذه البيانات يصدرها الكمبيوتر:

مسلسل	رقم الهاتف		المكان	الوقت	عدد الدقائق	السعر
	من	إلى				
1	7009894	7065432	جدة	8:06	12	50 ريال

وهذا معناه أن جهات الأمن تستطيع الحصول على كل مكالمات تليفونك في أي وقت من السنة.

وبالنسبة للهاتف النقال:

فإن جهات الأمن تستطيع بالإضافة إلى معرفة مكالماتك تحديد مكانك عن طريق الذبذبات التي يرسلها هاتفك النقال من وإلى البرج.

كيف تقوم الدولة بالتصنت العشوائي على المكالمات التليفونية للشعب؟

المكالمات التليفونية بالملايين في وقت واحد وهي في الهواء تماما مثل محطات الإذاعة فأنت عندما تفتح المذياع تسمع محطات و محطات و محطات..

نفس الشيء الدولة لديها أجهزة تصنت تسمى "متعدد القنوات " وهو عبارة عن جهاز كبير يقوم العامل فيه بإدارة قرص مثل قرص الراديو ويضع في أذنيه سماعات فيستمع إلى المكالمات التليفونية المختلفة التي تقدر بالآلاف مثل الراديو والعامل يتوقف ويتابع المكالمة، فإذا وجدها مكالمة عادية انتقل إلى مكالمة أخرى وهكذا.

إجراءات حماية الهواتف:

1) يفضل استخدام هواتف الشارع وعدم التحدث من البيت أو من الهاتف النقال أو من الفندق في حال السفر.

2) لا تورط هاتفك سواءً الثابت أو النقال في الاتصالات لأن الاستخبارات ستعرف على من اتصلت من خلال الفاتورة.

3) استغلال الفرص لتجنب الهواتف والتعويض عنها بالاتصال المباشر إذا أمكن.

4) يمنع منعاً باتاً نقل أي معلومة سرية على الهاتف إلا مشفرة وأستخدام الأسماء الحركية.

5) جعل المكالمة قصيرة لا تتعدى دقيقة واحدة ومن الأفضل كتابة المراد التحدث به قبل الاتصال.

6) عدم إعطاء أي بيانات لأي فرد يتحدث معك على الهاتف.

7) التفتيش عن أجهزة التصنت بصورة دورية.

8) تفقد حال الإخوة الذين يتم الاتصال عليهم عادة حتى لا يتم القبض على أحدهم وتستمر المخابرات باستقبال المكالمات في بيته أو عبر هاتفه النقال.

9) حفظ الأرقام ذهنيا أو تكتب بشفرة لا يفهم أنها أرقام تليفونات.

10) الرد على التليفون بصيغة متفق عليها بين أفراد المكان الموجود فيه لمنع حدوث أخطاء ترشد عن أسماء وطبيعة ساكني هذا المكان.

11) عدم جعل المكالمة مبهمةً وغامضةً، لأنه في هذه الحالة سوف يعتقد العامل أن هناك شفرة سرية أو أن هناك عملاً سرياً.

13) عدم ذكر من أين يتحدث الشخص، لا يذكر أسماء دول أو أماكن أحياء.

14) إذا كانت بلغة أجنبية وفي وقت قصير فإنها تكون أفضل لأن العامل قد يتجنبها.

15) عدم استخدام التليفون من قبل شخص معروف لدى الدولة أو سبق وأن رصد صوته لأنه يوجد الان لدى الحكومات نظام مراقبة بصمة الصوت.

5) الاتصال اللاسلكي - المخابرة أو ما يسمى بالآيكوم والكنود -

كفاءته ضعيفة ولا يعتمد عليه بالنسبة لغيره من الاتصالات.

- مزايا اللاسلكي:

1) شبكة اتصال خاصة لا تتوفر لأي نوع آخر.
2) يمكن الإبداع فيها لتؤدي مهمتها بأمان لمن يستخدمها.
3) يوفر عامل السرعة.

- عيوب اللاسلكي:

1) أسهل ما يمكن في الالتقاط والتحديد.
2) أسهل ما يمكن التشويش عليه.

- تأمين الاتصال اللاسلكي:

1) اختيار الجهاز المناسب ويكون حر التردد.
2) الجهاز المناسب للغرض المناسب - الجهاز حسب المدى المطلوب ولا يزيد كثيراً عنه -
3) تغيير الترددات والكود باستمرار.
4) اختيار الأفراد القائمين على الأجهزة بعناية ومراقبتهم.
5) اختيار شفرة مناسبة - للمكالمة أو الجهاز -

6) لمنع الالتقاط والتحديد يتبع الآتي:

أ) عدم الاتصال إلا عند الضرورة.
ب) عدم تحديد موعد الاتصال كموعد ثابت.
ج) تقليل مدة الاتصال قدر الإمكان.
د) استخدام أقل طاقة ممكنة للجهاز وتـؤدي الغـرض المطلوب.
هـ) استخدام هوائي موجه.

7) لمنع التشويش يتم اتباع الآتي:

أ) يتـم الاتصـال علـى ذبذبـة ثابتـة مـع وجـود ذبذبـة احتياطية متفق عليها بكود وليس صراحة بحيث يتم الانتقال إليها عند التشويش.
ب) تغيير مكان الاتصال كلما أمكن ذلك.
ج) عدم الاتصال يوميا.

8) اختيار عدة موجات ومراقبتها جيدا للتأكـد من عدم استخدامها من قبل أحد.

<u>ملاحظات:</u>

1) الإهمال في الاتصال باهظ الثمن تماماً.
2) الأتصـال اللاسـلكي - المخـابرة - خطـر جـداً ولا يستخدم إلا في الضرورة وبتشفير دقيق.

عن معسكر البتار
العدد الخامس / محرم
1425 هـ