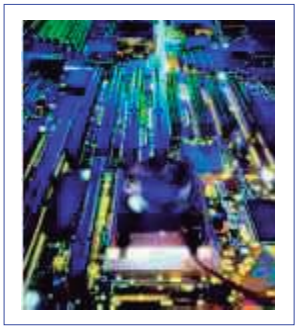
# Opine por Internet

Por Ricardo Ospina Bozzi
Alumno Cidenal

El correo electrónico puede convertirse en una herramienta muy práctica para generar opinión en favor de la Fuerza Pública. Sin embargo, hay que medir los riesgos y prevenirlos para que el mensaje sea más efectivo y seguro.



El Mono Jojoy aparece en televisión oyendo solicitudes de un grupo de secuestrados. Una emisora, la W FM, habla con familiares de secuestrados que no sabían de ellos desde hace mucho tiempo, y les da pruebas de supervivencia. El programa de televisión La Noche muestra imágenes de grupos de secuestrados. Ingrid Betancourt aparece en un video durante un noticiero. Mancuso concede una entrevista a la revista Semana...

Los escenarios anteriores tienen algo en común: las organizaciones delictivas necesitan que la población opine sobre estos asuntos, que los vuelvan tema obligado de conversación, que se llegue a las altas esfe-

# sin riesgos

ras. Todo, para llevar al gobierno y otros organismos internacionales a responder a sus propuestas de canje o de desmovilización... y los medios de comunicación les hacen el juego. Cada caso constituye una actividad de generación de opinión, en unos casos de las Farc y en otros, de las autodefensas.

El Estado colombiano y la Fuerza Pública también necesitan generar mensajes favorables a la causa y que expongan las actividades y reales intenciones de los grupos armados ilegales. Deben dar a conocer a la opinión pública nacional e internacional sus avances

# Opine por Internet...

y logros en la lucha contra el terrorismo y todas sus expresiones, y denunciar las actividades delincuenciales de estos grupos, como son el narcotráfico, el secuestro, la destrucción de pueblos, las masacres indiscriminadas contra la población, etc. Deben mostrar su progreso en el respeto por los Derechos Humanos y el acatamiento a las normas del Derecho Internacional Humanitario, sin dejar de mencionar el progreso técnico, los adelantos tecnológicos y su actual capacidad de reacción.

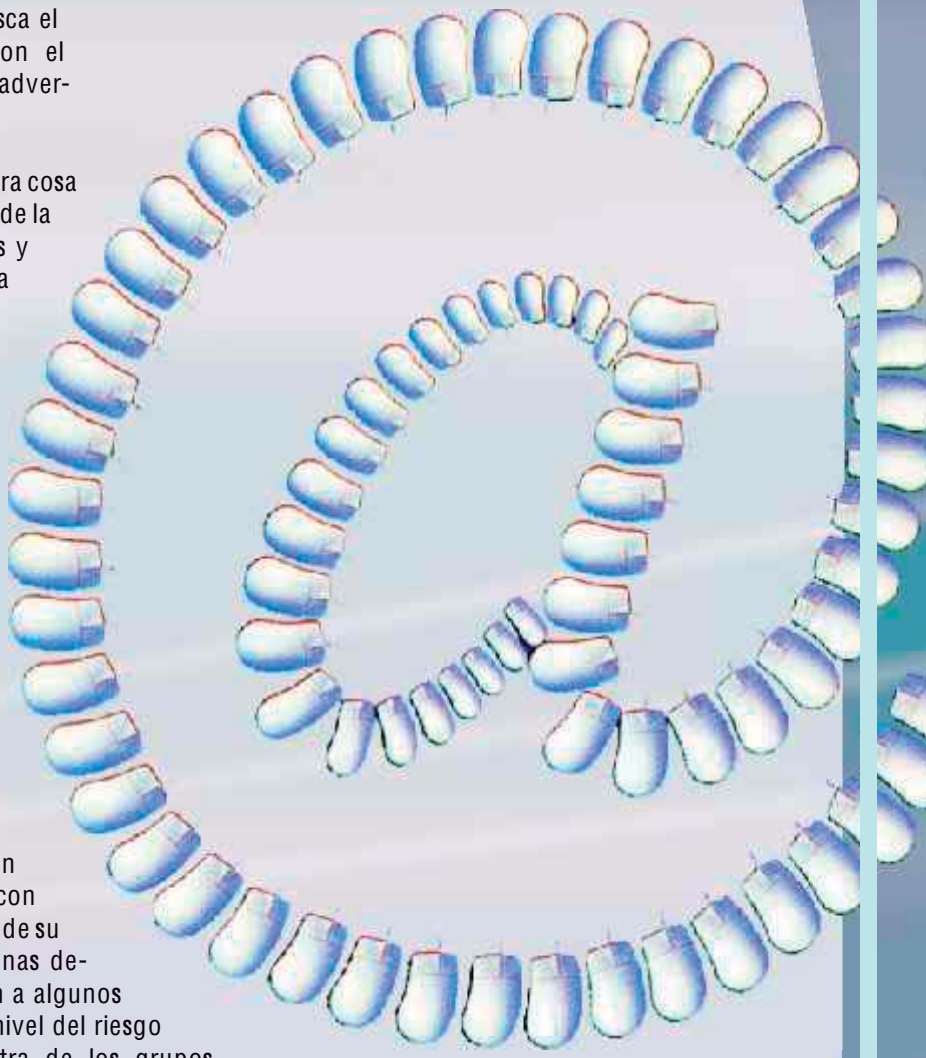
La transparencia en la difusión de información, su contenido y su veracidad son herramientas fundamentales para lograr el objetivo institucional de informar oportuna y seriamente a la comunidad.

La responsabilidad de llevar a cabo esta labor es de los comandantes, apoyados por las oficinas de comunicación y prensa y los departamentos de Acción Integral. Ellos, a su vez, necesitan la ayuda de otros grupos que estén en capacidad de difundir masivamente la información a través de columnistas, editoriales, directores de programas radiales o la simple comunicación escrita. En este sentido, muchos ciudadanos de bien han detectado la necesidad urgente de la Fuerza Pública de generar opinión a favor del Estado y de sus instituciones, y de contrarrestar la difusión de información de los grupos alzados en armas. Se han conformado así espontáneos grupos generadores de opinión conformados por civiles, quienes, sin pedir nada a cambio, realizan marchas de protesta contra los violentos, los secuestros, las mentiras... escriben a las revistas y los periódicos, llaman a las emisoras de radio y envían miles de mensajes de correo electrónico, generando opinión a favor de nuestro país y de nuestra Fuerza Pública.

Esta labor espontánea e incondicional de la ciudadanía ha cobrado relevante importancia en los últimos años, dada la necesidad de mantener a la opinión pública informada del acontecer nacional y del orden público. Una comunidad sin información o mal informada es un núcleo en potencia de conflictos, con el grave riesgo de que acepte la información suministrada por los grupos delictivos y generadores de violencia.

Esto cobra mayor importancia si se tiene en cuenta el principio de que en un conflicto como el que vivimos la actividad militar representa un 30 por ciento del esfuerzo, mientras que la acción integral representa el 70 por ciento restante. Y no se puede llevar a cabo acción integral sin generación de opinión, puesto que en su más elemental concepción, ésta busca el empleo máximo de propaganda integral con el propósito de minar la voluntad de lucha del adversario.

Puesto que la generación de opinión no es otra cosa que propaganda, la acción integral requiere de la primera para lograr su propósito en todos y cada uno de sus campos. ¿Qué sería de la acción sicológica, de la acción de masas, de la de estratagemas, de la de organizaciones, de la ideológica, de la acción informática, sin los grupos generadores de opinión encargados de diseminar la información?



Como el aporte del generador de opinión es definitivo para los resultados de la guerra, éste se involucra en ella, al punto que su seguridad personal o la de sus colaboradores podría estar en peligro. Esto es más cierto y más delicado cuando se trata de ciudadanos civiles, desarmados, que desinteresadamente quieren ayudar al país y que no cuentan con más protección que las paredes de su vivienda. Por ello, estas personas deberán poner especial atención a algunos aspectos que determinan el nivel del riesgo al generar opinión en contra de los grupos armados ilegales. Son dos los principales aspectos que se deben tener en cuenta cuando se envían mensajes que involucran de alguna forma a estos grupos:



sin riesgos

· El contenido del mensaje.
· Los destinatarios del mensaje, o blanco audiencia.

Dado que Internet es un nuevo medio de comunicación, con un altísimo potencial en la generación de opinión y con la gran ventaja sobre medios tradicionales de que democratiza el acceso a éstos y ofrece la posibilidad de opinar e informar a cualquier persona, conviene que los ciudadanos generadores de opinión y los militares que usan este medio tomen medidas para reducir los riesgos a su seguridad e integridad.

## NIVELES DE RIESGO

Para comenzar, vale la pena establecer el nivel de riesgo en que se incurre al enviar un mensaje, el cual depende, como ya se mencionó, del contenido y del blanco audiencia o destino final del mismo. Los niveles se clasifican en alto, mediano y bajo riesgo, dependiendo del grado de compromiso que el mensaje pueda causar a la seguridad del remitente.

El contenido puede causar riesgo cuando crea compromisos de responsabilidad al remitente. Por otro lado, el blanco audiencia o destino del mensaje causa riesgo en la medida que éste se componga de individuos no afectos o con tendencias hacia los grupos armados ilegales.

## NIVEL DE RIESGO ALTO

Se refiere al riesgo causado por mensajes que de una u otra forma pueden crear una situación de peligro para el remitente, particularmente cuando se trata de civiles que actúan en defensa de los intereses nacionales y que con esta actividad afectan los de los grupos subversivos.

Un mensaje se considera de alto nivel de riesgo cuando reúne simultáneamente condiciones como las siguientes:

· Que su contenido comprometa de alguna forma al remitente, su familia o su equipo de trabajo, como es el caso de mensajes que contengan graves acusaciones o denuncias, fundadas o no, que involucren a grupos subversivos o sus organizaciones.
· Que entre los destinatarios se incluyan individuos o grupos que pertenecen a grupos ilegales o simpatizan con ellos.

## NIVEL DE RIESGO MEDIO

Se considera como nivel medio aquél que sólo incorpora una de las dos condiciones anteriores, es decir, aquel mensaje en el que o bien el contenido compromete al remitente, o bien el destinatario puede ponerlo en peligro.

## NIVEL DE RIESGO BAJO

Un bajo nivel de riesgo es aquél en el que no se cumple ninguna de las condiciones enunciadas: el contenido del mensaje no compromete la seguridad del remitente o sus allegados, y tampoco está dirigido a grupos delincuenciales o a sus afectos.

## REDUZCA EL RIESGO Y AUMENTE LA EFECTIVIDAD

De la misma forma que la propaganda, la generación de opinión puede ser blanca o gris. Es blanca cuando la fuente se identifica plenamente, es decir, el receptor conoce el origen del documento. En estos casos, si la fuente es la Fuerza Pública, el documento puede considerarse oficial. Es gris cuando se deja a la imaginación del destinatario la identificación del remitente.

Para lograr mayor efectividad de sus mensajes, es preferible hacer uso de la generación de opinión blanca siempre que se pueda, pues produce mayor credibilidad. Sin embargo, a mayor credibilidad, mayor riesgo para usted, si la información es sensible y afecta los intereses del enemigo.

Se puede hacer generación de opinión gris cuando no se desea que se conozca que es usted el remitente del mensaje. En este caso, puede usar una cuenta de correo con un nombre que no lo identifique. El contenido de su mensaje perderá fuerza, pero es la mejor alternativa para disminuir el nivel de riesgo.

En cuanto a sus destinatarios, usted tiene varios posibles receptores de sus mensajes:

· Militares y civiles colaboradores generadores de opinión.
· Población civil afecta.
· Población civil desafecta.

# Internet...



· Grupos armados ilegales o miembros de ellos.

En los primeros dos casos, es posible que usted se encuentre ante un mensaje de bajo nivel de riesgo (excepto si el contenido es comprometedor), mientras que en los dos casos siguientes es probable que se encuentre en un nivel medio o alto. Sin embargo, conviene tomar precauciones adicionales con el caso de la población civil afecta, y considerar un nivel de riesgo medio, ya que no se sabe en realidad quién recibirá su mensaje, bien sea directamente o por redireccionamiento de alguien más.

Recuerde que no sólo reciben su mensaje aquéllos a quienes se les envía, sino también quienes lo reciben de estos últimos. Revisemos entonces cada uno de los posibles destinatarios.

**La transparencia en la difusión de información, su contenido y veracidad son herramientas fundamentales para lograr el objetivo institucional de informar oportuna y seriamente a la comunidad.**

## RESPETO A MILITARES Y CIVILES COLABORADORES COMO DESTINATARIOS

Al enviar mensajes a estos grupos, nunca presente las direcciones de correo en el campo que va visible para quien recibe. Es decir, no las ponga en el campo para, ni en el campo copia (To y Cc, en los sistemas en inglés).

Las direcciones de los militares y civiles generadores de opinión deberán ir siempre en el campo de copia oculta, o Cco (en español) o Bcc (en inglés). Cuando usted abre un nuevo mensaje, no aparece el campo para la copia oculta. Por ello, debe seleccionar el campo para, y cuando aparezca la lista de su libreta de direcciones, seleccione los destinatarios que desee y haga clic sobre Cco o Bcc. Una vez escogidos todos los destinatarios, pulse aceptar.

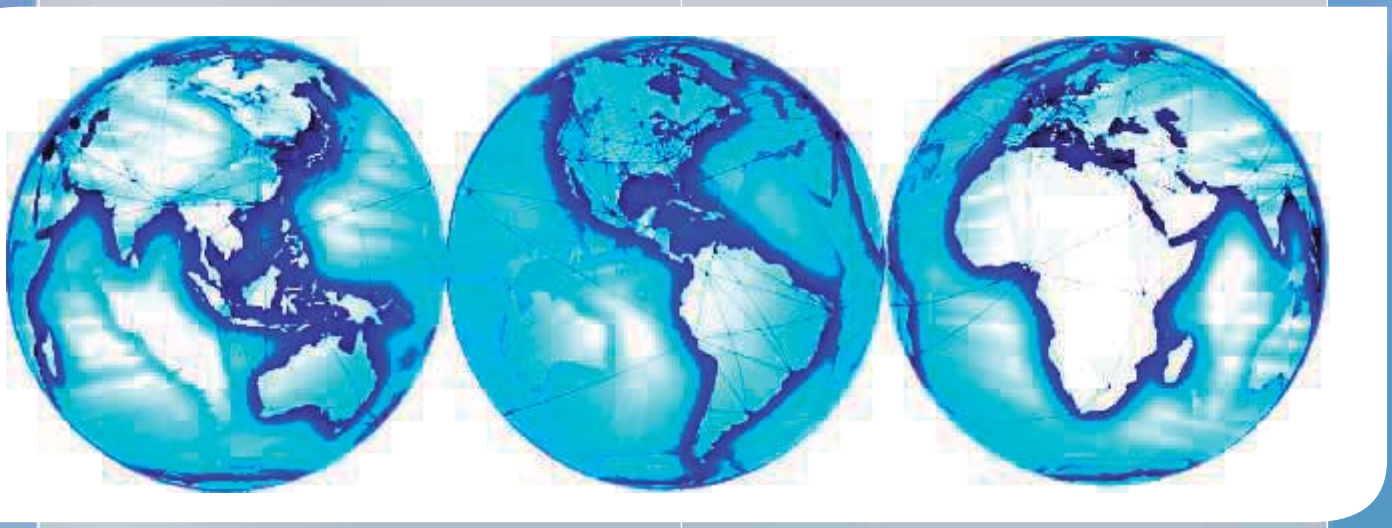
En el campo para, puede escribir su propio nombre y dirección. El remitente envía el mensaje para sí mismo, con copias ocultas a sus destinatarios reales, que en este

# Opine por

caso son propias tropas o colaboradores.

Hay varios motivos de seguridad para poner las direcciones en el campo de copia oculta, Cco:

· Si los destinatarios son visibles y el adversario recibe uno de estos mensajes, contará con las direcciones electrónicas de sus hombres. Entonces, podrá hacerle contrainteligencia, desinformarlo, etc.
· Un mensaje puede ser retransmitido tantas veces, de nombres o direcciones en los campos Para y Copia son desagradables a la vista de quien los recibe.
· En caso de retransmitir su mensaje, se irá con filas interminables de nombres y direcciones en el cuerpo del mismo, que lo hacen desagradable de leer. O, de lo contrario, el destinatario intermediario deberá borrar los nombres o direcciones antes de reenviarlo. Si las direcciones van ocultas, quien retransmite sólo tendrá que borrar la dirección del remitente.
· Es desagradable para quien recibe, pensar que es



que puede salirse de su control el destinatario final. A la larga, usted nunca sabrá quién recibió ese mensaje, y si las direcciones de los destinatarios originales son visibles, tampoco sabrá quién tiene las direcciones de sus hombres.
· Si el adversario recibe mensajes con destinatarios visibles, podrá introducir su propia dirección entre ellos y contestarles. Los destinatarios replicarán desprevenidamente el mensaje entre sus conocidos (por ejemplo, un chiste), creando una cadena en la que la dirección del adversario va incluida. Eventualmente, éste formará parte del grupo y podrá enterarse de sus actividades, movimientos y operaciones, porque recibe copias de la correspondencia.

Hay otros motivos para usar copias ocultas que, si bien no son de seguridad, es importante tener en cuenta:

· Por presentación, pues un mensaje que viene lleno

simplemente uno más de una lista de correo.
· A los piratas informáticos (hackers) les fascinan los mensajes de correo electrónico con muchas direcciones a la vista, pues ellos pueden capturarlos y utilizarlos para sus propósitos.
· Los comerciantes de bases de datos usan estos mensajes mal dirigidos para obtener y vender direcciones electrónicas.

RESPECTO A POBLACIÓN CIVIL AFECTA COMO DESTINATARIO

Se aplican las mismas consideraciones anteriores para propias tropas para evitar los casos presentados anteriormente y que el enemigo obtenga sus direcciones y les haga operaciones sicológicas a través de ellas, y además para que el destinatario no sienta que lo maltrata al incluirlo en listas de correo electrónico y tratarlo como uno más.

En casos de población civil afecta, tenga la precaución

sin riesgos

# Internet...

de que puede haber desafectos dentro de la lista, disfrazados o sin su conocimiento.

Una consideración adicional, más de presentación que de seguridad, pero que causa un mejor impacto en los receptores del mensaje, es tratar de bautizar a todo el grupo de destinatarios con un mismo nombre. Por ejemplo, si el mensaje va para periodistas, llame a todo el grupo "Señor periodista"; si va para senadores, "Honorable Congresista"; o a un grupo de conocidos, "Amigos". Para hacerlo, entre a la libreta de contactos y cree un nuevo contacto que se llame con el nombre del grupo. Asigne a este contacto su propia dirección. Cuando envíe el mensaje, anote este nombre en el campo para y las direcciones reales del grupo en el campo de la copia oculta.

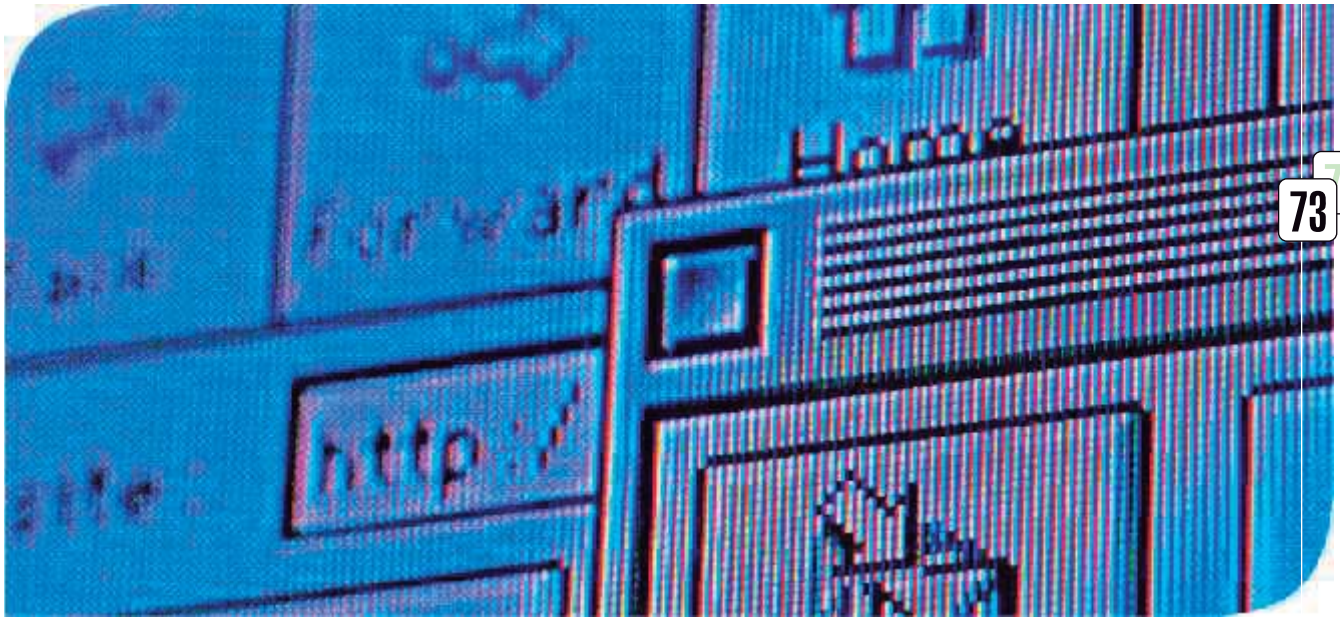
Si se verifican las propiedades de la dirección "Honorable Senador", se encontrará que corresponden a la dirección del remitente del mensaje, pero el mensaje será recibido por todo el grupo de destinatarios.

## RESPECTO A POBLACIÓN CIVIL DESAFECTA Ó EL ADVERSARIO COMO DESTINATARIO

Estos son mensajes con clasificación de riesgo medio y alto, por lo que se deben tomar algunas precauciones de seguridad. Para comenzar, asuma las mismas condiciones de seguridad expuestas hasta el momento, de manera que no se corran riesgos de entregar información sobre sus colaboradores.

Cuando se comunique con población desafecta o con el adversario, tenga presente que su programa de correo anexa a su mensaje una gran cantidad de información sobre usted. La más importante es el número de Protocolo de Internet (dirección IP) utilizado por su computador, así como los datos de su servidor de acceso a Internet. Siendo ésta la situación, usted deberá considerar varios detalles:

**Para lograr mayor efectividad de sus mensajes, es preferible hacer uso de la generación de opinión blanca siempre que se pueda, pues produce mayor credibilidad. Sin embargo, a mayor credibilidad, mayor riesgo para usted, si la información es sensible y afecta los intereses del enemigo.**



# Opine por internet...

· Al generar opinión gris, no use el mismo computador que usó haciendo generación de opinión blanca. Si comete este error, corre el riesgo de descubrirse, ya que el destinatario podrá verificar que ambos remitentes tienen acceso al mismo equipo y que probablemente se trata de la misma persona.

· En el mismo sentido, si usted hace generación de opinión blanca, no debe usar el mismo equipo de quien genera opinión gris.

· Si el destinatario tuviera acceso a su proveedor de internet, podría averiguar quién es usted. Así lo hacen las autoridades para atrapar a los hackers. Así que cualquier previsión para no entregar esta información, como utilizar proveedores alternos, debe ser considerada en caso de mensajes de alto riesgo.

Conociendo el potencial y a la vez los riesgos de los mensajes de correo electrónico, usted podrá expresarse con mayor tranquilidad y evitará exponerse y exponer a sus colaboradores y familiares. No hay que temer a estos riesgos, simplemente prevenirlos y aprovechar la red mundial de computadores para que, junto a miles de colombianos, generemos opinión en favor de nuestro país y de nuestra Fuerza Pública.