The Information Leader

Summer 2007
Volume 12, No. 3

A Quarterly Journal on Information Trends by the World Leader in Information Resources Management Education

Terrorists and the Internet

By Irving Lachow and Courtney Richardson

Cyberterrorism conjures images of infrastructure failures, economic disasters, and even large-scale loss of life. It also receives a great deal of coverage in the press. While the threat of cyberterrorism is real, the hype surrounding the issue often outpaces the magnitude of the threat. In addition, the term itself deflects attention from a more mundane but equally serious problem: terrorist organizations effectively using the Internet to stymie U.S. efforts to win the Long War.

The Internet enables terrorist groups to operate as either highly decentralized franchises or freelancers. Similar to information age businesses, these groups use the Internet to create a brand image, market themselves, recruit followers, raise capital, identify partners and suppliers, provide training materials, and even manage operations. As a result, these groups have become more numerous, agile, and well coordinated, all of which make them harder to stop. Furthermore, these groups have become expert at using the Internet to manipulate both public opinion and media coverage in ways that undermine American interests. In short, rather than attacking the Internet, terrorists are using it to survive and thrive.

This article examines why the Internet is so useful for terrorist organizations. It then considers how terrorists use the Internet for strategic advantage and why the threat of cyberterrorism may be overstated in many cases. The article concludes with a set of observations and recommendations.

Why the Internet?

The Internet has five characteristics that make it an ideal tool for terrorist organizations. First, it enables rapid communications. People can hold conversations in real time using instant messaging or Web forums. Instructions, intelligence information, and even funds can be sent and received in seconds via email. Second, Internet use is a low-cost proposition. Terrorist organizations can now affordably duplicate many of the capabilities needed by modern militaries, governmental organizations, and businesses: a communications infrastructure, intelligence-gathering operation, training system, and media-savvy public affairs presence. Third, the ubiquity of the Internet means that small terrorist groups can have a global cyber presence that rivals that of much larger organizations. Terrorists not only can communicate with each other from almost anywhere in the world, but they also can create a Web site that is viewed by millions and possibly even examined daily by media outlets for news stories. Fourth, the growth in bandwidth combined with development of new software has enabled unsophisticated users to develop and disseminate complex information via the Internet.

For example, in December 2004, “a militant Islamic chat room posted a twenty-six minute video clip with instructions on how to assemble a suicide bomb vest, along with a taped demonstration of its use on a model of a bus filled with passengers.” Finally, modern encryption technologies allow Internet users to surf the Web, transfer funds, and communi-

(Continued on page 2)

Contents

IRMC Information Resources Management College

The IRM College is a global learning community for government’s most promising information leaders.

National Defense University

Terrorists and the Internet (cont.)

(Continued from page 1)

cate anonymously—a serious (though not insurmountable) impediment to intelligence and law enforcement organizations trying to find, track, and catch terrorists. To achieve anonymity, terrorists can download various types of easy-to-use computer security software (some of which is commercial and some of which is freely available) or register for anonymous email accounts from providers such as Yahoo! or Hotmail.

Internet as Strategic Tool

The combination of characteristics described above makes the Internet a valued strategic asset for terrorists. In fact, one could argue that the Internet, along with other modern communications technologies, is a *sine qua non* of the modern global extremist movements. Successful terrorism requires the transformation of interested outsiders into dedicated insiders. Once someone has become an insider, less intense but still continuous interactions are required to maintain the needed level of commitment to the cause.

Before the advent of advanced communications technologies, this process was entirely based on face-to-face interactions which limited the scope of a given group. The Internet, however, allows groups to create and identify dedicated insiders—and to maintain fervor in those already dedicated to the cause—on a global scale. Advanced technologies also allow the extremists to deliver well-coordinated propaganda campaigns that increase the levels of support among the general public, which in turn allows terrorists to operate freely in these societies. For example, one of al Qaeda's goals is to use the Internet to create "resistance blockades" in order to prevent Western ideas from "further corrupting Islamic institutions, organizations, and ideas." One technique they use is to distribute Internet browsers that have been designed to filter out content from undesirable sources (for example, Western media) without the user's knowledge.

In summary, the development and proliferation of the Internet have enabled the rise of loose, decentralized networks of terrorists all working toward a common goal. In the words of one expert, "it is the strategic—not operational—objectives of the jihadi movement's use of technology that engenders the most enduring and lethal threat to the United States over the long term."

Cyberterrorism?

It is evident that terrorist groups are extremely effective in using the Internet to further their missions. Are they also using, or planning to use, the Internet to launch a major cyber attack on the United States? We do not know, but there are a number of factors that suggest the answer to this question is no. Terrorism, by definition, is focused on obtaining desired political or social outcomes through the use of tactics that instill fear and horror in target populations.

Cyberterror can be defined as: *a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples. . . . Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.*

History shows that the vast majority of cyber attacks, even viruses that cause billions of dollars of damage to an economy, are not going to cause the levels of fear desired by most terrorists. In comparison, using physical means to create terror is fairly easy and quite effective. Put in these terms, it is not surprising that terrorists prefer to inflict damage with physical means and then use the Internet to magnify the results of their handiwork. Indeed, while there is clear evidence that terrorists have used the Internet to gather intelligence and coordinate efforts to launch physical attacks against various infrastructure targets, there has not been a single documented incidence of cyberterrorism against the U.S. Government.

One could argue that terrorists would use the Internet to attack cyber assets that control physical systems, thereby creating horrific physical effects via cyber means. The most likely scenario of this type is an attack on the control systems that manage parts of the Nation's infrastructure (for example, dams, trains, and power plants). The consequences of an attack of this kind would be serious, so this threat deserves attention. However, the actual likelihood of such an attack is unknown; different analyses have reached different conclusions.

(Continued on page 3)

(Continued from page 2)

Two things are certain: successfully launching such an attack would not be easy, and the consequences are difficult to predict due to the incredible complexity and interdependence of critical infrastructures. Given a choice of conducting either a cyber attack with unknown consequences or a physical attack that is almost certain to cause graphic deaths that will create fear, it is understandable why terrorists have (so far) chosen the latter.

Observations

Terrorists use the Internet to harm U.S. national security, but not by attacking infrastructure or military assets directly. Instead, terrorists use the Internet to improve their operational effectiveness while simultaneously undermining our military and diplomatic efforts to win the war of ideas. There is little doubt that they are doing both things well. While there is a possibility that they may use the Internet to launch a cyberterror attack against American targets, this threat falls under the broad umbrella of critical infrastructure protection—a topic that is getting a great deal of attention at all levels of government. This issue is not addressed here. Rather, the focus rests on the other two uses of the Internet—issues that are equally important but often receive comparatively less focus, energy, and resources.

Terrorist Operational Effectiveness. The Internet enables terrorist organizations to operate as virtual transnational organizations. They can use it to raise funds, recruit, train, command and control, gather intelligence, and share information. Clearly, it is in the U.S. interest to either disrupt or undermine these activities. The good news is that relying on the Internet is a double-edged sword for terrorist organizations: despite the many benefits associated with using the Internet as their main intelligence, command and control, and communications system, this approach carries a few liabilities. Terrorist reliance on Web sites and discussion forums allows outsiders to monitor their methods and track trends. For example, there are groups such as the SITE Institute that focus on monitoring terrorist Web sites and providing information to a wide range of interested parties, including elements within the U.S. Government. Reliance on the Internet also creates the opportunity for outsiders to pose as insiders in order to provide misinformation or simply to create doubt among the terrorists about whom they can trust.

To that end, the United States should make every effort to infiltrate extremist virtual communities in order to gather intelligence and begin planting the seeds of mistrust that can disable terrorist cells. We presume that governmental activities of this kind are under way. Surprisingly, nongovernmental organizations appear to contribute to these efforts as well. For example, individual citizens have infiltrated terrorist networks via chat rooms and then worked with governmental agencies to bring about several arrests.

The bad news is that terrorists are doing their best to minimize the liabilities associated with heavy reliance on the Internet. They are quick to learn from mistakes and to disseminate best practices on how to defeat the tactics used by intelligence and law enforcement agencies. Terrorist groups are adept at quickly moving their Web sites from host to host, which makes them difficult to track and shut down (trusted members of these groups use chat rooms, email, and other forums to share information about the new location of a moved site). They also like to masquerade some activities as legitimate business operations.

Terrorist Influence Operations. One of the most difficult challenges facing the United States is countering terrorist use of the Internet to propagate their ideological agenda. This problem is part of the much broader war of ideas against the extremist Islamic movement. Efforts to date have not proven successful, as evidenced by the following statement from former Secretary of Defense Donald Rumsfeld: "If I were grading I would say we probably deserve a 'D' or a 'D-plus' as a country as to how well we're doing in the battle of ideas that's taking place in the world today." This is a complex issue that does not lend itself to easy answers.

Recommendations

U.S. efforts to influence must be tied to real-world actions. While it is easy to focus on the principles of effective communications strategies, our words will ring hollow if they are not related to the realities experienced by the target audience. Thus, it goes without saying that what the United States does is as important, if not more so, as what it says. To that end, diplomatic and military influence operations must ensure that target audiences are aware of the positive actions undertaken by the United States in the Muslim world, while simulta-

(Continued on page 6)

Building Security into Software: An Acquisition Official Perspective

By Mary Linda Polydys and Stan Wisseman

This is an abridged version of an article which appeared in the May 2007 issue of CrossTalk, a journal on Defense Software Engineering. The title of the article is "Software Assurance: Five Essential Considerations for Acquisition Officials."

There is a growing concern that acquisition officials are not aware of their responsibility to build in Software Assurance (SwA) into software services and products and reduce the risk of exploitable software being passed to users. To address this concern, a guide entitled "Software Assurance in Acquisition: Mitigating Risks to the Enterprise" (https://buildsecurityin us-cert.gov) was developed on how to incorporate SwA considerations in key decisions throughout the acquisition process.

This article provides a summary of five essential SwA considerations that acquisition officials should include in their decision-making. These considerations are extracted or synthesized from the acquisition guide which provides more detailed discussion and explanation along with additional considerations.

SwA considerations should be included in each phase of the acquisition process from the initial acquisition strategy and plan, requirements development, contract or purchase, and contract administration through follow-on software support efforts. The objectives of these SwA considerations are to ensure the delivery of reliable software that functions as promised and software free from security vulnerabilities and malicious code.

Essential Consideration #1 – Build Security In: Create Acquisition Strategies and Plans That Include Essential SwA Considerations

To build security in, SwA considerations should be planned from the inception of a software or software-intensive system acquisition through delivery and post-release support. The Federal Acquisition Regulation (FAR) requires that an acquisition plan be developed for all acquisitions and that all plans discuss how agency information security requirements are being met. The Defense Acquisition Guidebook requires program managers to develop an Acquisition Information Assurance (IA) Strategy as part of their Acquisition Strategy. Whether developing a strategy or plan in accordance with the FAR, Defense Acquisition Guidebook, or another directive, SwA should be part of the discussion on how information security requirements are to be met. To that end, the strategies or plans might include a discussion on the participation of SwA subject matter experts in the acquisition process, initial SwA risk considerations, plans for including SwA requirements, SwA considerations in contractor selection, and SwA considerations in contract administration and project management.

Acquisition officials should require the participation of SwA subject matter experts in the acquisition process from planning, requirements development, source selection, contract award through contract administration, and project management. This is essential not only for establishing appropriate SwA requirements, but also in evaluating potential contractors and ensuring that secure software is delivered. Acquisition strategies and plans should state the level of SwA expertise required as well as specific statements of involvement.

Strategies and plans should include an initial discussion on risk management. For information assurance/security, the security category (SC) (based on a range of risk levels) should be included in strategies and plans. The Federal Information Processing Standard Publication (FIPS Pub) 199 as mandated by the Federal Information Security Management Act (FISMA) of 2002 requires that a security category be designated for each software-intensive system. The DoD Instruction (DoDI) 8500.2 provides security categorization rules for DoD software-intensive systems using Mission Assurance Categories (MAC) and confidentiality levels. The FIPS Pub 199 states that security categories should be based on the mission that the software is to support, the environment in which the mission is performed, and, generally, the kind of information that is generated and maintained to support the mission (e.g., medical, privacy, classified, time sensitive, warfighter combat information, financial, security management, etc.). Security categorization includes an assessment of three security objectives defined in FISMA: confidentiality, integrity, and availability.

Acquisition strategies and plans should include statements of critical, high-level SwA considerations. These high-level statements guide the ultimate detailed statement of requirements. Acquisition officials developing acquisition strategies and plans should rely heavily on the SwA personnel assigned to the acquisition. High-level statements on how SwA is to be considered in the selection of contracts should also be included in acquisition strategies and plans. As an example: Due diligence questionnaires will be used to solicit answers from offerors on their SwA practices. The answers will be part of the evaluation plan.

Lastly, high-level statements should be included in acquisition strategies and plans on how SwA requirements are to be monitored during contract performance, for example: SwA personnel will monitor the delivery of SwA requirements.

Essential Consideration #2 – Require Secure Software: Include SwA Requirements in Software Requirements Document

The security category is the basis for SwA requirements. The

(Continued on page 5)

(Continued from page 4)

FAR requires that Federal agencies use FIPS pubs for IT standards and guidance. The FIPS Pub 200 includes guidance on minimum security requirements for federal information and information systems. The National Institute for Standards and Technology Special Publication (NIST SP 800-53) provides specific security control requirements based on security category, and the DoDI 8500.2 contains security control requirements based on mission assurance category for the DoD. The guide for acquisition officials includes additional sources for SwA requirements, as well as some examples.

Essential Consideration #3 – Be an Educated Consumer: Ask the Right Questions During the Contracting Process

Knowing what to ask and asking the right questions regarding offerors' SwA environments is essential in determining how well offerors meet business and technical goals for SwA. The guide for acquisition officials includes sample software due-diligence questionnaires for various types (e.g., COTS only, software integration services, software development, etc.) of software acquisitions. These questionnaires provide the acquisition official a means to gather, in advance, some of the information needed to make a decision about whether it offers the process capabilities to deliver reliable software that functions as promised and software free from security vulnerabilities and malicious code.

Essential Consideration #4 – Demand Delivery of Secure Software: Ensure SwA Requirements Are Met During Contract Administration and Project Management

Acquisition officials should ensure that all the SwA requirements are adequately monitored and implemented. This includes work plan management, assurance case management, software risk management, and final acceptance of the software product or service.

Acquisition officials must ensure that SwA requirements are specifically included in a contract work plan and/or work breakdown structure, if required. SwA subject matter experts should be used to ensure that SwA requirements are included in the work plan.

Five Essential Software Assurance (SwA) Considerations for Acquisition Officials:

1. *Build Security In: Create Acquisition Strategies and Plans That Include Essential SwA Considerations*
2. *Require Secure Software: Include SwA Requirements in Software Requirements Document*
3. *Be an Educated Consumer: Ask the Right Questions During the Contracting Process*
4. *Demand Delivery of Secure Software: Ensure SwA Requirements Are Met During Contract Administration and Project Management*
5. *Continue SwA for the Life of the Software: Maintain SwA in Follow-On Support*

Acquisition officials must ensure that the SwA case is managed in accordance with the contract and should be managed as part of the acquisition risk management strategy. The development of an SwA case is an iterative process throughout a system's life cycle and contains a plethora of claims and evidence types not collated or contained together. Therefore the SwA case must be developed and managed in such a fashion that all evidence is able to be preserved, traced, and accessed. Throughout the acquisition life cycle, SwA case reports – as stipulated in the contract – should be delivered at key project milestones. These reports should be reviewed by appropriate SwA subject matter experts for issues and recommendations. Acquisition officials must ensure that periodic reviews of the SwA case are transparent and any corrective actions are followed to a conclusion prior to acceptance of the case argument. Example issues related to SwA case management during contract performance include the following:

- Performance. Is the SwA case development progressing in accordance with contract requirements? Are project technical milestones incorporating SwA case review? Does the SwA case comply with contract requirements, including regulations and certification requirements?

- Resources. Has the contractor allocated appropriate, qualified personnel to the task? Is the SwA case being developed with appropriate tools? Is the SwA case budget realistic?

- Quality. Is the supplier engaging the right acquisition officials to review the acceptability of the SwA case? Are corrective actions being followed up adequately? Are the contractor's claims, arguments, and evidence sufficiently robust and commensurate with risk?

- Time. Is the SwA case development on schedule and fully integrated with software system development?

Final acceptance should be based on the acceptance of the final SwA case. Criteria for acceptance should be explicit and included in the SwA case.

(Continued on page 6)

Building Security into Software (cont.)

(Continued from page 5)

Essential Consideration #5 – Continue SwA for the Life of the Software: Maintain SwA in Follow-On Support

Follow-on support is the logistics tail in the acquisition of software. Additional contracts are often awarded to provide support during this phase. There should be ongoing analyses to ensure that security requirements remain adequate. To that end, acquisition officials should ensure that the assurance/security requirements implemented and accepted in previous contracts flow to the follow-on contract efforts. Additionally, acquisition officials should ensure that contract language is in place to guide the transition process from an incumbent contractor to a new contractor responsible for follow-on support.

Weak change/configuration control procedures can corrupt software and introduce new security vulnerabilities. Therefore, acquisition officials should ensure that strong change/configuration control flows to follow-on contract efforts.

Patches and upgrades make direct changes to software and potentially the configuration of the operating system to which they are applied. Changes may degrade performance, introduce new vulnerabilities, or reintroduce old vulnerabilities. In order to understand patch risks, the patch process must be examined in some detail during the initial acquisition and again when follow-on support contracts are awarded. One of the most common patch failures stems from a lack of encryption and authentication in the implementation phase. Suppliers should provide updates in a secure fashion. There should be no doubt that the source is legitimate and the update's integrity is maintained in transit.

In conclusion, large numbers of vulnerable software-based systems exist today, in many cases due to the acquisition of vulnerable software. The rampant, worldwide increase in exploitation of software vulnerabilities demands that acquisition officials not only check for acceptable functionality, but also achieve acceptable SwA. Security cannot be bolted on after software services and products are delivered. To that end, acquisition officials must become educated consumers in the purchase of secure software, and each phase of the acquisition process must be leveraged to build security in to ensure the delivery of reliable software that functions as promised and software free from security vulnerabilities and malicious code.

The full version of this article is found at: http://www.stsc.hill.af.mil/CrossTalk/2007/05/ 0705PolydysWisseman.html

Terrorists and the Internet (cont.)

(Continued from page 3)

neously highlighting the negative actions of our enemies.

The corollary to this point is that the United States must effectively get its story out before the terrorists or insurgents can use the Internet to spin events in their favor. It is much harder to respond to or discredit initial stories, even ones that are untrue, than to establish the baseline facts or perceptions in the first place. There are certainly elements of the U.S. Government making heroic efforts in this area. For example, the Department of State maintains a Web site in a number of languages (including Arabic, Farsi, and French) that is devoted to countering false stories that appear in extremist sources. It also focuses on countering disinformation likely to end up in the mainstream media. U.S. Embassies have used this resource to counter disinformation in extremist print publications in Pakistan and elsewhere. There are also military units deployed overseas that are exhibiting best practices in operational level influence operations. Unfortunately, much work remains to be done for such examples to become the rule rather than the exception.

A related point is that the Nation must view the war of ideas as equal in importance to the military and law enforcement aspects of the war on terror. The war-of-ideas aspect of any decision involving the Long War must be considered at the highest levels of U.S. policymaking. That emphasis must then be communicated down the chain so that all players understand the importance of message in this war. Strategic communications cannot be seen as an afterthought of a military operation or as the sole responsibility of an office buried within the State Department. The recent announcement that the Office of the Secretary of Defense is creating a new office focused on strategic communications is a move in the right direction. Similarly, information operations cannot be viewed simply as a set of activities done by a local commander in support of tactical objectives. It is clear from past experience that such approaches are not effective in the long run if they are not tied to strategic considerations.

Countering terrorist use of the Internet to further ideologi-

(Continued on page 7)

(Continued from page 6)

cal agendas will require a strategic, government-wide (interagency) approach to designing and implementing policies to win the war of ideas. For example, to counter terrorist influence operations, all Federal agencies should use the same specific and accurate language when referring to Salafist extremists. It is of the utmost importance that American policymakers set their terms of the debate. Expressions such as jihad and mujahideen are part of the popular lexicon describing antiterrorist operations in Iraq, Afghanistan, and elsewhere. However, such terms disempower the United States. Jihad literally means "striving" and is frequently used to describe every Muslim's responsibility to strive in the path of God. Mujahideen is closely translated to mean "holy warriors." Such a term may have worked to U.S. advantage in Afghanistan against the Soviet Union—however, terms such as these now pit the United States as the enemy against holy warriors in a holy war. Rather, terms such as hirabah ("unholy war") and irhabists ("terrorists") should become part of the popular lexicon.

As important as it is for the United States to improve its own communications efforts, a key part of countering extremist misinformation and propaganda is to have messages come from a variety of sources—preferably some of them local. For example, it is critical for the United States to promote the views of well respected Muslim clerics, who counter the claims made by Islamic terrorists and extremists. Such efforts have been undertaken by the government of Saudi Arabia, but American efforts in this area have been lacking. In effect, the Nation should do everything possible to enable moderate Muslims to develop a strong, vibrant, and responsive Internet and media presence of their own.

Terrorists use the Internet to harm U.S. national security interests, but not by conducting large-scale cyber attacks. Instead, they use the Internet to boost their relative power to plan and conduct physical attacks, spread their ideology, manipulate the public and media, recruit and train new terrorists, raise funds, gather information on potential targets, and control operations.

Last but not least, resources must be made available to support all of these efforts, plus others such as training and education to improve understanding of Muslim cultures and languages spoken within these cultures. Current U.S. resources dedicated to strategic communications, public diplomacy, and information operations are woefully inadequate. On the military side, the lack of training and education in information operations at all levels—strategic, operational, and tactical—often requires commanders to learn on the job and build information operations teams "out of hide." While some leaders will certainly rise to the occasion, this approach is not a recipe for success in a complex, media-heavy war against adversaries who are highly adept at conducting their own influence operations.

Terrorists use the Internet to harm U.S. national security interests, but not by conducting large-scale cyber attacks. Instead, they use the Internet to boost their relative power to plan and conduct physical attacks, spread their ideology, manipulate the public and media, recruit and train new terrorists, raise funds, gather information on potential targets, and control operations. If these activities can be curtailed, then the viability of the terrorist groups themselves may be put into question. To that end, the United States needs to focus more resources into two areas: countering the operational effectiveness associated with terrorist use of the Internet, and undermining Internet-based terrorist influence operations. If it can successfully meet these two challenges, the United States will make significant progress toward winning the Long War.

References are available upon request.

Podcasting Made Easy

By Les Pang

This article is divided into two parts—first, how to create an audio podcast and, secondly, how to create a video podcast for situations where you and your audience have access to video iPods.

How to Create an Audio Podcast

A podcast is an audio file you can create and upload to a server. Your intended listeners download your audio file so they can listen to it at their convenience on their own iPod or MP3 player. If they want they could "subscribe" to your podcast via iTunes and "RSS" technology so they can retrieve the latest episodes.

Quick Start Directions

You will need a computer with a microphone (most laptops have a microphone already built-in). Your computer should have the Flash player (typically it is already loaded if you have a recent version of Internet Explorer) and iTunes so you can download the podcast to your iPod.

You will set up an account at http://www. podomatic.com where you will create both your first podcast "episode" (an episode represents a single "show" in a collection of "shows") and a web page which includes links to your episodes. You may record anything in your podcast (a simple greeting or short interview will do). It will be saved on the podOmatic server and you will have the opportunity to tell others about your podcast. Listeners can download your podcast episode and sync it to their iPod. Using iTunes, listeners can also subscribe to the podcast.

Detailed Directions

1. Preparation

Skip this step if you already have a working microphone installed with your computer.

It is a good idea to have a quality microphone, but you might start out with something inexpensive – your local computer store sells them for under $15. Of course, laptops often have microphones already built-in.

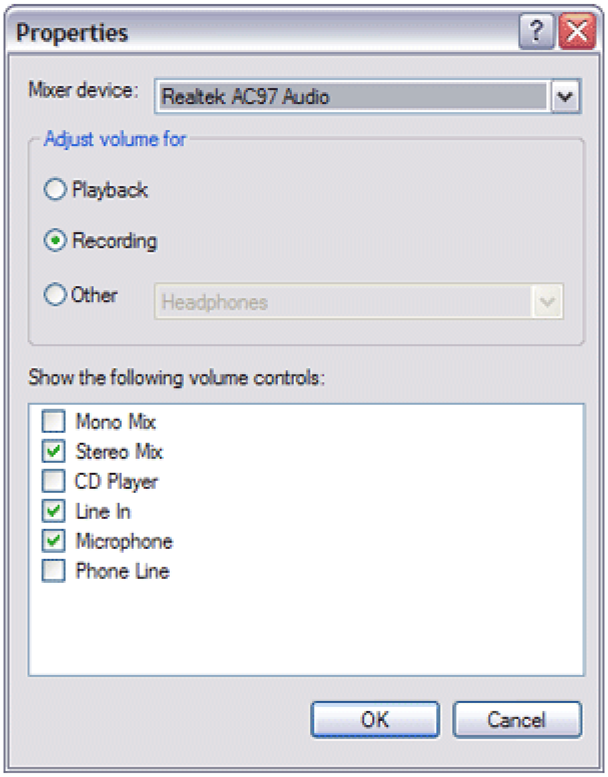
Headphones are helpful because you need to monitor the levels of your recording but you don't want to have the sound coming from a set of speakers being recorded by the microphone. It is best to have headphones that cover your ears to isolate sound in your recording from other audio distractions, but ear bud headphones may also do the trick.

a. Connect the microphone to the microphone-in connection on your PC.

b. Connect your headphones to the stereo line out or headphone jack. This is often the same jack.

c. Either double-click the speaker icon in the system tray or go to **Start > Settings > Control Panel > Sounds and Audio Devices**. In the **Device volume** section, click the **Advanced…** button.

d. With the Volume Control open choose **Options > Properties** from the menu and click the button next to **Recording**. Make sure the controls are selected as shown below. Click **OK**.



Properties

Mixer device: Realtek AC97 Audio

Adjust volume for

○ Playback

● Recording

○ Other Headphones

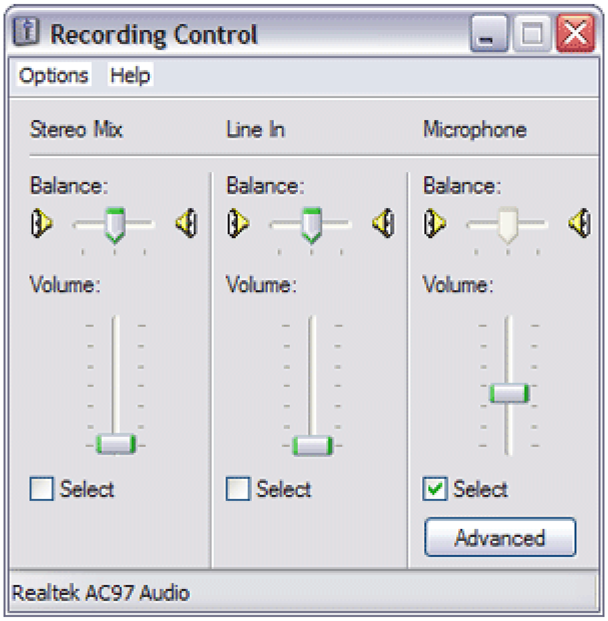
Show the following volume controls:

□ Mono Mix
☑ Stereo Mix
□ CD Player
☑ Line In
☑ Microphone
□ Phone Line

e. Returning to the Recording Control window, make sure the Microphone is selected and the volume for the Microphone is above zero or you won't be recording anything (see below). Leave

(Continued on page 9)

the Recording Control open so you can make adjustments during the recording process.



2. Recording Your Podcast

If you plan to use Internet Explorer as your browser, you will need to allow the QuickTime program to run.

From your browser, access http://www. podO-matic.com. This is a free service (a premium version is also available) that lets you record a podcast (*or video-cast!*) directly to the Web. It uses Flash to access a PC's microphone and video camera.

a. Click “Signup” to create an account as a podO-matic user. Select an identifying photo if you wish. Click “**Post your first episode**.” Provide the requested information – title of your podcast episode (e.g., Welcome to My First Podcast), tags (keywords for searching for your podcast episode) and Comments.

b. In recording your first podcast episode, consider a simple welcome, a commentary or you can get fancy and do an interview with someone else. Keep it short for your first try -- about 1-2 minutes. BTW, podOmatic can hold up to 500MB (1 minute of a MP3 file is about 2 MB). Allow the program to access your microphone. Click the **Record** button and stop when done. Click **Preview** (Note: Often the playback is of poor quality and seems shortened but go ahead and use it anyway. Also, the playback does not automatically stop – you must stop it.). You do have the option of re-recording if necessary.

Note: If you have problems recording while in podOmatic, go to the Troubleshooting section below.

Next, select **Post Episode**. The episode will be uploaded to a server.

c. You will be given an opportunity to share your podcast. You can **Skip** these windows if you wish.

3. Getting the Word Out via the Podcast Web Page

After your podcast is created, select **My Podcast Page**. You are on your web page that lists the podcast episodes you created. (It may take a few minutes for your latest episode to appear particularly if it is large size – try the **Refresh** button occasionally.)

4. Downloading to Your iPod

Still on your podcast web page, select **Download**. Chose **File, Save As** and save the MP3 file in the “My Music” folder. Next sync your iPod so that your podcast will be loaded on your device. After connecting your iPod to the computer, select the Podcasts tab, click the Sync checkbox and choose your podcast. Click the **Apply** button.

5. Subscribing to Your Podcast

Return to the **My Podcast** page (http://www. podO-matic.com/podcast). Locate the RSS URL -- it is right after “Your RSS Feed” on the top of the page (it looks something like: http://lpang10473.podOmatic.com/rss2.xml). Copy this RSS URL to the Clipboard.

Next, open iTunes and select **Advanced > Subscribe to Podcast**. Paste the RSS URL from the Clipboard. This will allow access to all of the new episodes of the podcast.

(Continued on page 10)

Podcasting Made Easy (cont.)

(Continued from page 9)

Double-click on your podcast in iTunes to listen to your latest episode as an RSS feed.

6. Final Notes

a. During a later session, you can add another episode by logging in, going to **My Podcast** and choosing **Post an Episode**. The new episode will appear above the previous one on your podcast web page.

b. You can add an embedded podOmatic player for a web page. Visit: http://www.podomatic.com/podcast/embed

Congratulations, you have completed your first podcast!

Samples of Podcasts

http://lpang10473.podomatic.com
http://dshughes76.podomatic.com/
http://tigerbabe.podomatic.com/
http://liebsterindahouse.podomatic.com/
http://armystrong.podomatic.com/

Troubleshooting

If you have trouble recording while in the podOmatic web site, you can (1) separately record your podcast using a sound editor program, (2) convert it to MP3 format then (3) import it within the podOmatic site.

1. You can download a free sound program called Audacity (http://audacity.sourceforge.net/) then record your podcast.

2. Next you will need to download the MP3 decoder (such as LAME) to convert your podcast file to an acceptable format.

   Go to: http://www-users.york.ac.uk/~raa110/audacity/lame.html

   Click on any link from the list of identical "lame-3.96.1" links.

   When you have finished downloading LAME, unzip it and save the file **lame_enc.dll** anywhere on your computer.

   Return to Audacity. The first time you use the "Export as MP3" command, Audacity will ask you where lame_enc.dll is saved. Proceed with the export function and create your MP3 file.

   An alternative to this approach is to use Microsoft Sound Recorder -- which you already have as a Windows utility -- to record your podcast. Next, you have to download an MP3 encoder such as Media Monkey (http://www.mediamonkey.com/) and convert the WAV file (generated by Sound Recorder) to MP3 format.

3. Now that you have an MP3 file, go into the podOmatic web site and **Post an Episode**. Instead of recording in podOmatic, use the **Import** function.

How to Create an Video Podcast

Similar to an audio podcast, a video podcast is a movie file that you can share with others and they can subscribe to your podcasts to get the latest episodes.

Quick Start Directions

You will need a computer and a digital video camcorder such as miniDV camcorder. Your computer should have the Flash player (typically it is already loaded if you have a recent version of Internet Explorer) and iTunes so you (and others) can download the podcast to an iPod.

Videotape a short clip using your camcorder. Attach the camera to your computer and capture the movie using Windows Movie Maker (this video editing program comes with Windows). Edit the movie as needed then save as a wmv file. This movie will become your video podcast.

If you haven't already, you need to set up an account at http://www.podOmatic.com where you can upload your video podcast "episode" (an episode represents a single "show" in a collection of "shows") and create a web page which includes links to your episodes.

Import (i.e., upload) your video to the podOmatic server and you will have the opportunity to share with other your podcast. Listeners can download your podcast episode and sync it to their iPods. Using iTunes, listeners can also subscribe to the podcast.

(Continued on page 11)

(Continued from page 10)

Detailed Directions

1. Record and Edit Your Video

Using your digital video camcorder, record a short clip (2-3 minutes) for this first try. Consider a simple welcome or you can get fancy and do an interview or a tour of your home or office.

Attach your camcorder to your computer (typically using an IEEE1394/Firewire/DV connection) and turn it on.

If prompted, select the option to capture the video using Windows Movie Maker. If not prompted, run Windows Movie Maker (**Start > Programs > Accessories > Entertainment**) and select **Capture from video source**.

After capturing the video, Movie Maker automatically divides your video into segments to make it easier to drag and drop the parts you want onto the Storyboard (bottom of the window) where you put your movie together.

You'll see your clips in the Collections view. Click on each clip to see how it looks in the Preview window (on the right). Click the Play button.

Once you've decided which ones you want to put in your movie, click and drag the clips down to the Storyboard in the order in which you'd like them to appear in your final movie. (If you don't see the Storyboard as shown below, click **Show Storyboard**.)

You can do a lot in Movie Maker such adding titles, transitions, special effects and so on. You might want to consult: http://www.microsoft.com/windowsxp/using/moviemaker/default.mspx

When you have created a final version of your podcast, select **File > Save Movie File**. Save it to "My Computer." Give it a descriptive name and make sure that it is saved in the **My Videos** folder. It will be saved in WMV format. Save the file as Best Quality.

Before exiting Movie Maker, you will want to select **File, Save Project** to save this Movie Maker project in case you want to go back and work on editing the movie later. It is saved as a MSWMM file. Edit this file and not the WMV file if you want to make changes.

2. Uploading Your Podcast

From your browser, access http://www.podOmatic.com which lets you upload audio or video directly to the Web.

a. If you haven't yet, click "Signup" to create an account as a podOmatic user.

b. Go to **My Podcast** and select "**Post your first episode**" or **Post an Episode.** Provide the requested information – title of your podcast episode (e.g. Welcome), tags (keywords for searching for your podcast episode) and comments.

c. Click the **Import** button. Right of "upload", click **Browse**, locate the WMV video file you created earlier using Movie Maker. It should be in the **My Videos** folder.

Next, select **Post Episode**. Note the progress bar -- the episode is being uploaded to a server. If it's a long video, it will take a few minutes. (A 40 MB video takes about an hour to upload.)

After the upload, you will then get a message that your file is being converted to the appropriate format. Later, you will get an e-mail when the conversion is complete.

(Continued on page 12)

Podcasting Made Easy (Cont.)

(Continued from page 11)

Note: You have the option of podOmatic taking control of your connected camcorder then do the recording. However, the author never got this to work properly.

d. You will be given an opportunity to share your podcast. You can press **Skip** to bypass these windows if you wish.

3. Getting the Word Out via the Podcast Web Page

After your podcast is created, select **My Podcast Page**. You are on your web page that lists the podcast episodes you created. (It may take a while for your latest video episode to appear – you will get an e-mail when it is done.)

4. Downloading to Your iPod

Still on your podcast web page, select **Download**. Chose **File, Save As** and save the video file in the “My Video” folder. Next sync your iPod so that your podcast will be loaded on your device. After connecting your iPod to the computer, select the Podcasts tab, click the Sync checkbox and choose your podcast. Click the **Apply** button.

5. Subscribing to Your Podcast

Return to the **My Podcast** page (http://www. podOmatic.com/podcast). Locate the RSS URL -- it is right after “Your RSS Feed” on the top of the page (it looks something like: http://lpang10473. podOmatic.com/rss2.xml). Copy this RSS URL to the Clipboard.

Next, open iTunes and select **Advanced > Subscribe to Podcast**. Paste the RSS URL from the Clipboard. This will allow access to all of the new episodes of the podcast.

Double-click on your podcast in iTunes to listen to your latest episode as an RSS feed.

6. Final Notes

a. During a later session, you can add another episode by logging in, going to **My Podcast** and choosing **Post an Episode**. The new episode will appear above the previous one on your podcast web page.

b. You can add an embedded podOmatic player for a web page. Visit: http://www.podomatic.com/podcast/embed

Now that you know how to create both an audio and video podcast you can use this medium to deliver quality content that your audience will enjoy and appreciate!

“The views expressed in this publication are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government.”

INFORMATION RESOURCES MANAGEMENT COLLEGE

The World Leader in
Information Resources Management Education

300 5th Avenue Marshall Hall (Building 62)
Fort Lesley J. McNair, DC 20319
(202) 685-2096
http://www.ndu.edu/irmc/
GET ISSUES ONLINE: http://www.ndu.edu/irmc/out_infott.htm

Director: Dr. Robert Childs
Dean of Faculty & Academic Programs:
Dr. Elizabeth McDaniel
Editor-in-Chief: Dr. Les Pang
Associate Editor: Dr. James Kasprzak
Banner: James Looney