DIGITAL RESISTANCE
Course on Digital Security

Gaziantep, Turkey
14 – 16 January 2014

Course Report: Assessment and Lessons Learned
1. **Background and mandate**

The “Digital Security Training - digital resistance” was organised by No Peace Without Justice (NPWJ) together with the Local Administration Council Unit (LACU), a branch of the Syrian National Council (SNC), the Violations Documentation Center (VDC), the Kirkayak Art Center (KSM) and Front Line Defenders. The training took place from 14 to 16 January 2014 in the city of Gaziantep, where a number of international NGOs and international organisations have been based since the start of the Syrian crisis. No Peace Without Justice’s Syria Project Coordinator and digital security expert, Mr Hadi Al Khateeb, shared his expertise with 9 participants.

Digital security is essential, for those who are working on the ground and those who are collecting and preserving sensitive data abroad. The risk of becoming a victim of digital attacks by specialised intelligence units is increasing, with the consequent danger of losing data and revealing information about sources and witness identities.

The training aimed to introduce participants to a correct and safe documenting process which is the first way to ensure an effective accountability process for the perpetrators that committed crimes.

Specific objectives of the training included a digital threat assessment, analysis of the importance of passwords and an introduction to antivirus and anti-malware devices and software.

The course provided hands-on experience of all these tools with the support and guidance of Mr al Khateeb. It offered participants the chance to learn different techniques and strategies to safeguard digital communications, including encryption, safe document storage and the management of sensitive data. Moreover the participants were provided with a *digital security pack* with open source applications to help secure personal computers and networks, together with handbooks and manuals such as security in a box,¹ to ensure continued protection after the training.

Concrete examples from the Syrian conflicts and practical exercises were used to illustrate the best practices and lessons learned to help improve digital security awareness among Syrian human rights activists and media officers inside Syria.

This three-day training course is part of an NPWJ transitional justice project aimed at reducing the expectation and rewards of impunity and at building a culture of accountability. One particular goal is to strengthen Syrian civil society in the prevention of sexual and gender-based violence, particularly against women and children, as well as challenging impunity for such crimes. The overall purpose is to equip citizens to demand accountability and justice for violations taking place on a daily basis for the past two and a half years and, at the same time, to equip the judiciary and legal profession to answer that demand.

The mainstay of the project is a series of advocacy and training events, which are being held in Gaziantep, Turkey, near the Syrian border, with Syrian judges, lawyers and civil society activists from Syria who can bring the skills and (perhaps more importantly) aspirations for justice back to their work and their constituents inside Syria.

The long-term goal of this project is to promote democracy and human rights protection through incorporating justice and accountability in decision-making on conflict resolution and stability, development, and reconstructing planning in Syria. The project’s strategic objective is to support Syrian civil society playing an active role on justice and accountability issues, including advocacy and documenting human rights violations, including receiving, gathering, collecting, collating, processing and securely storing information, documentation and materials and analyse it for the purpose of establishing what happened and reconstructing decision-making processes that resulted in violations of international humanitarian and human rights law in Syria since March 2011.

---

¹ NPWJ is grateful to Tactical Technology Collective for having produced these excellent tools, which are highly recommended. For more information, see www.securityinabox.org and https://tacticaltech.org/.
2. Course Summary

2.a Participation
The Course on Digital Security was attended by 9 participants. The participants included media officers and human rights activists from LACU, VDC, Local Councils and representatives of informal associations both from inside Syria, from Aleppo, Damascus, Homs and Hama, and based in Turkey. During the training, Syrian journalists from local media outlets also attended the sessions as observers and covered the course.

2.b Presenters
The presenter for the Training Course was NPWJ’s Syria Project Coordinator, based in Gaziantep, who is also an expert of the specialised areas addressed by the course.

Hadi Al Khateeb
Before joining NPWJ, Hadi Al Khateeb worked with Tactical Technology Collective for the security and protection of rights advocates. From 2006 to 2010, he worked in the protection field with various international organisations in the Middle East including Medicins Sans Frontieres and the Danish Refugee Council. His work has focused on maintaining strong relationships with community groups and coordinating resources to meet organisational and project needs. He holds a bachelor’s degree in economics from the University of Tishreen, Syria.

2.c Training program
The content and format of the Training Course curriculum was developed by NPWJ in co-operation with the training partners, based on previous experiences on this field and the background of participants. The final course program is attached to this report and shows the full range of topics covered by the Training Course.

In the opening session of the first day of training, Mr Al Khateeb welcomed the participants for their participation and presented the NPWJ project and the program of the course, its content, agenda, logistics and practical information. Participants were asked to present themselves and their respective roles and expertise related to digital security and to describe their expectations with regard to this training.

The first session focused on an overall understanding of the risks and threats related to the management of digital information, underlining vulnerabilities and capacities of different IT tools. This session highlighted the important of an effective risk assessment of the dangers related to IT communications in order be able to put in practice effective defensive actions that can help prevent hacking or loss of information. Mr Al Khateeb continued in the next session to deepen the theoretical framework on digital security, focusing on defining some of the most important sources of threats: malware, spyware and viruses, tackling also the framework of social engineering. The session ended with some practical demonstrations and exercises to explain how to protect computers, mobile phones and social media pages from possible threats and digital attacks. Mr Al Khateeb underlined how to make sure that computers and other devices are not vulnerable to hackers or plagued by malicious software, often called malware, such as viruses and spyware. This is a basic but useful precaution, otherwise it would be impossible to guarantee the effectiveness of any other security strategy. In the last session, the participants learned about issues related to malware and viruses and used different up-to-date open source software provided by NPWJ staff members and distributed on USB flash.
Mr Al Khateeb explained how to maintain software and how to use tools like Avast, Spybot and Comodo Firewall to protect computers against the dangers of malware infection and hacker attacks. The Digital Security Pack provided during this session included handbooks and manuals, both in Arabic and English, looking at digital security and focused on tools and strategies that can be used to avoid censorship.

The second day was devoted to topics related to the creation of effective and secure passwords and the correct storage of sensitive data on digital tools. The presenter and participants engaged in a discussion on the main difficulties faced by human rights activists in Syria and the strategies they have been implementing to overcome those challenges. During the second session, the presenter developed practical exercises, highlighting how secret words, phrases or strings of gibberish often provide the first, and sometimes the only, barrier between stored information and anyone who might want to read, copy, modify or destroy that information without the owner’s permission. Participants and the presenter discussed the techniques to destroy and erase sensitive data from hardware and laptops and how to restore any loss of information. Each new method of storing or transferring digital information tends to introduce several new ways in which the information in question can be lost, taken or destroyed. Years of work can disappear in an instant, as a result of theft, momentary carelessness, the confiscation of computer hardware, or simply because digital storage technology is inherently fragile. It is extremely important to create and conserve an up-to-date backup and be aware of a well-tested means of restoring it. On the other hand, the presenter underlined the importance of a permanent and safe erasure of files. In order to ensure that deleted information does not end up in the wrong hands, people should use special software made especially for this, which was presented by the presenter. The next session focused on digital communication and file sharing. In a world where networking is the basis of communications, storing data in a safe way is not enough. Unfortunately, the alternatives to traditional means of communication cannot always be relied upon to keep sensitive information private: postal mail, telephone calls and text messages are all also vulnerable, particularly when used by those who may have been targeted for surveillance by the authorities. Taking certain precautions, the flexibility of Internet communication tools and the strength of modern encryption can now provide a level of privacy that was once available only to national military and intelligence organisations.

On the third day, the group of participants analysed in detail secure browsing techniques and the importance of privacy settings in social media and websites. Regardless of what filtering methods are present, it is nearly always possible to evade them by relying on intermediary computers, outside your country. This process is often called “censorship circumvention”, or “simply circumvention”, and intermediary computers are called proxies. Proxies, too, come in many different forms.

At the end of the last session, presenter and staff of No Peace Without Justice thanked the participants for their presence and active participation. The presenter thanked them for taking the risks associated with coming to Gaziantep to engage in this training and expressed the hope that their expectations may be fulfilled and that they will find the possibility to share their experience with their colleagues inside Syria and to put their knowledge into effective practice. Mr Al Khateeb noted the commitment of No Peace Without Justice in supporting participants’ efforts in disseminating the information learned and shared, by fostering the communication network with participants through Skype and social media. He ensure that a network among presenter and participants will be established and participants are welcomed to keep NPWJ informed about their future initiatives and to express interests for future training topics to NPWJ staff. NPWJ is committed to provide further assistance according to their needs and activities. Participants expressed their gratitude to the Frontline defenders and No Peace Without Justice for the very useful information obtained, and committed to apply their acquired knowledge in the field. Participants filled out the overall evaluation form for the training, in addition to the daily evaluation forms, to allow NPWJ to improve future courses. Each participant received the certificate of attendance and USB sticks with documentation provided.
3. Assessment and Recommendations

Since the start of the Syrian revolution three years ago, internet activism and digital documentation of human rights violations have been the main networking tools among activists engaged in organising peaceful protests. At the same time, in reaction to the repression committed by regime forces and to the isolation of Syrian civil society, internet has played a key role for documenting the ongoing violations and is often the only tool to take and preserve testimony about what has been happening inside Syria. Due to the high importance that digital communications has in Syria, it is a priority of NPWJ to assist human rights activists that use high technology techniques on a daily basis in learning how to protect themselves and how to minimise the risk of being tracked in their activities, to promote democracy, freedom of expression and accountability.

There were, as anticipated, lessons to be learned in terms of what if implemented will strengthen future training programs in terms of their participation, role of presenters and content and structure of the course program.

3.a. Participation

In this training, nine participants attended the program; unfortunately, unlike other NPWJ training courses, no women took part in this course. NPWJ should continue to support wider female participation and promote the active role of women within society. The participants were either members of VDC or media officers of the Syrian local councils, based both in Syria and in Turkey. All participants involved had background relevant to the training content and were working in the collection, documentation and reporting of human rights violations, be it as documenters, journalists, photographers or media officers. From a geographical point of view, six participants were based in Turkey while three came from the cities of Idlib, Homs and Hama.

Practical exercises and concrete reference to the Syrian context contributed to the excellent participation and interaction among the group of participants and presenter. The limited number of participants and the training course in Arabic allowed the establishment of a direct relationship and dialogue, where active participation and interaction were promoted during the whole course. Coffee breaks and meals were good occasions to continue the discussion on political aspects of certain strategies to control the digital communications used by the regime and offered the chance for NPWJ staff to understand better the real threats that participants are experiencing and facing directly.

Recommendations:

− Increase active promotion of female presence during the trainings, both with partner organisations and during participant selection processes;
− Ensure effective follow up with participants through advanced trainings on digital security as well as developing a way so the presenter is able to send tips and advices regarding digital security.

3.b. Presenters

The presenter was of the highest quality and experienced in the issues under discussion. Thanks to his previous experience in the field of digital security in many different countries, but always with a special reference to the Syrian case, he was able not only to deliver very technical information but also to provide participants with concrete references to their daily experience and threats. Holding the course entirely in Arabic enhanced the interactive experience among the group. To address the need for further courses of this kind, further regular but smaller and more targeted courses will be organised in the coming weeks.
Recommendations:
- Prefer experts who can speak Arabic, to enhance the interactive experience among participants.
- Ensure follow up with participants and assist them in the consolidation of the new techniques learned.
- Follow up with participants to develop possible raising awareness campaigns inside Syria.
- Follow up with participants to do a TOT so they can train other activists on security issues inside Syria.

3.c. Training Program

The Training Course curriculum was based on specific requests coming from Syrian partners and the presenter designed the program to cover relevant issues of digital security and protection, safe data storage and management and useful open source applications to secure computers and data. Future training courses should continue to build on this model but with advanced information, keeping most of its elements and making some improvements based on lessons learned.

Participants and presenter agreed that the exercises are fundamental part of the program and participants pointed out that there was a good balance of theory and practice.

Recommendations:
- Ensure follow up activities, both with participants and the presenter, in order to organise new activities and follow-up projects on the ground.
- Foster networking among participants to ensure coordination and information exchange.
- Make sure that presentations in power point are all translated into Arabic.
- Raise funds to buy original Windows 7 operating system and Anti-virus programs to distribute to activists during the training. Also make sure to present Free and Open Source operating systems such as Ubuntu.
- Work on TOT materials in Arabic to teach digital security so participants can use it to do trainings inside Syria.
- Make sure to have VPN accounts for participants.
- Design a security training for Android phone users as it is the most device used to take photographs in Syria.
- The training should be in Arabic.

3.d Answers to “what was the most useful session for you?”
- Lesson was good, especially encryption software for files.
- Practical sessions on how to install and use the tools.
- Data encryption software and save passwords.
- Email encryption.
- Clarify the technical and encryption mechanisms in general.
- How to create and save files and passwords of all kinds of practical and theoretical applications.
- How to encrypt files and store them on different devices.
- Knowing open source software.
- Chat encryption.
3.e Answers to “on what topics would you like more training in the future?”
- Programs on the security side.
- Email encryption.
- How to encrypt terabytes of data and keep it online.
- Training of trainers on digital security.
- Mobile phone security.
- How to archive information online in a secure way.
ANNEX 1

Training summary course program:
DIGITAL SECURITY TRAINING – DIGITAL RESISTANCE -

Day 1 - Tuesday, 14 January: 10:00 to 17:00

10:00-11:00: Opening session
  • Introduction and overview of the course
  • Introduction of participants & expectations
  • Logistics information about the training

11:00-11:30: Coffee Break

11:30-13:00: DIGITAL SECURITY RISK ASSESSMENT
  • "Security" and "digital security'';
  • Understanding the risks;
  • Definition of the threats, vulnerabilities and capacities;
  • Practical exercise for assessing the risks.

13:00-14:30: Lunch Break

14:30-15:30: DIGITAL PROTECTION
  • What are viruses, malware and spyware;
  • Dangers and threatens caused by viruses, malware and spyware (with case studies relevant to Syrian activists);
  • Social Engineering;
  • How to protect your computer from viruses, malware and spyware (part I).

15:30-16:00: Coffee Break

16:00-17:00: DIGITAL PROTECTION
  • How to protect your computer from viruses, malware and spyware (part II);
  • Importance of keeping your software up-to-date and the use of open source softwares;
  • Practical tips against viruses and malware;
  • Conclusions and evaluation.

17:00-17:30: daily wrap-up
Day 2 – Wednesday, 15 January: 10:00 to 17:00

10:00-11:00: SECURE PASSWORDS AND PROTECTION (Part I)
   • Dangers and threats caused by weak passwords (with case studies relevant to Syrian activists);
   • How to create and maintain secure passwords.

11:00-11:30: Coffee Break

11:30-13:00: SECURE PASSWORDS AND PROTECTION (Part II)
   • Practical exercise of passwords creation, protection and management.

13:00-14:30: Lunch Break

14:30-15:30: HOW TO PROTECT SENSITIVE DATA ON YOUR COMPUTER (Part I)
   • How to remove hidden meta data from files (practical exercise);
   • How to destroy sensitive information (practical exercise);
   • How to recover from information loss (theory and practice);
   • How to protect files on your computer (practical exercise).

15:30-16:00: Coffee Break

16:00-17:00: HOW TO PROTECT SENSITIVE DATA ON YOUR COMPUTER (Part II)
   • Sensitive data transfer (practical exercise);
   • Secure file sharing;
   • Conclusions and evaluation.

Day 3 – Thursday, 16 January: 10:00 to 17:00

10:00-11:00: PROTECTION OF PERSONAL COMMUNICATIONS ON INTERNET
   • Overview of how internet works
   • Secure browsing;
   • Protecting your electronic mail, social networks and other applications (practical exercise).

11:00-11:30: Coffee Break

11:30-12:30: PROTECTION OF PERSONAL COMMUNICATIONS ON INTERNET
   • Secure instant messaging (practical exercise).

13:00-14:30: Lunch Break
14:30-15:30: **HOW TO REMAIN ANONYMOUS AND BYPASS CENSORSHIP ON INTERNET**

- Overview on the concept of censorship;
- How to remain anonymous and bypass censorship on internet (practical exercise).

15:30-16:00: **Coffee Break**

16:00-17:00: **HOW TO PROTECT YOURSELF AND YOUR DATA WHEN USING SOCIAL MEDIA**

- Social engineering (hacks to Syrian activists through social media);
- Privacy on social networks;
- Safer alternatives (email and social networks);

Conclusions and evaluation.
ANNEX 2
PARTICIPANT LIST

For security reasons, the complete list of participants and their names cannot be published. The participants represented different organisations: Violations Documentation Center (2), Local Councils (6) and the Syrian National Coalition (1). Participants included documenters, photographers, video makers and media officers.

<table>
<thead>
<tr>
<th>Location of Participants</th>
<th>Type of activism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aleppo</td>
<td>Human rights activist, works at Aleppo Local Council</td>
</tr>
<tr>
<td>Aleppo</td>
<td>Human rights activist, works at Aleppo Local Council</td>
</tr>
<tr>
<td>Antakya</td>
<td>Works with the Violation Documentation Center and media activist</td>
</tr>
<tr>
<td>Damascus countryside</td>
<td>Media activist</td>
</tr>
<tr>
<td>Hamah</td>
<td>Human rights activist, works at Hamah Local Council</td>
</tr>
<tr>
<td>Homs</td>
<td>Media activist and lawyer</td>
</tr>
<tr>
<td>Istanbul</td>
<td>Works with the Syrian National Coalition</td>
</tr>
<tr>
<td>Istanbul</td>
<td>Works with the Local Administration Councils Unit on one of their databases</td>
</tr>
<tr>
<td>Nizib camp</td>
<td>Works with the Violation Documentation Center</td>
</tr>
</tbody>
</table>

Observers
Ms Ishraga Mustafa (Human rights investigator, International Commission of Inquiry on Syria).

Presenter
Hadi Al Khateeb