**Investigation Consideration**

**Chimene tchokoko diboma**

**Assignment**

**9 Oct, 2019**

*“Table of Contents”*

[*Introduction 3*](#_Toc422916763)

[*step 2 6*](#_Toc422916764)

[*step 3 5*](#_Toc422916765)

[*step 4 7 Toyata Motor 10*](#_Toc422916766)

[**Organizational structure** 11](#_Toc422916767)

[CIA 12 Quality 15](#_Toc422916774)

[Cyber threats  12](#_Toc422916775)

**Solution 15**

[CONCLUSION AND RECOMMENDATIONS](#_Toc422916793)

BIBLIOGRAPHY

**1. Introduction**

The initiation of a criminal case is the first stage of the criminal process in which the interrogating officer, the body of inquiry, the investigator and the prosecutor accept and verify the statement or report of a committed or preparing crime and, within the competence established by the criminal procedure code, decide on the need for a preliminary investigation on criminal case in connection with the availability of sufficient data indicating signs of a crime, or the refusal to initiate a criminal case, or the transfer of the application on jurisdiction and the criminal cases of the private prosecution - to the court.

The criminal prosecution stage precedes the preliminary investigation stage. Its main task is to provide a quick response to every crime and create the opportunity for a comprehensive, complete and objective study of all the circumstances of the incident. A criminal case should be instituted in every case where there is at least the smallest chance that a crime has been committed. From the moment the case is opened, the criminal prosecution the mechanism is put in place, and the body of inquiry, the interrogating officer, investigator or prosecutor are given the opportunity to use all methods and means prescribed by law to ensure the rights and legitimate interests of citizens and establish objective truth (Maguire, M. (2003).

The interaction of investigators (interrogators) with the bodies of inquiry is determined by objective premises, the most important of which, according to A.P. Derbeneva, are as follows:

* the community of their tasks in the fight against crime;
* the difference of authority;
* the specificity of forces, means, and methods of combating crime;
* the independence of the investigator and the body of inquiry, resulting from the lack of administrative subordination to each other

A prosecutor, as well as an investigator or interrogating officer, shall have the right to initiate a criminal case with the consent of the prosecutor. Moreover, the adoption of such a decision is not only the right of these bodies, but also their obligation: a case must be instituted in each case of detecting signs of a crime. The investigator has the right to petition the prosecutor to initiate a criminal case when information about the crime came directly to him or when he himself discovered signs of a crime (for example, during the investigation of another crime). Usually, they initiate cases under his jurisdiction on tribal and territorial grounds.

**1.1 Purpose of the planning**

The purpose of planning in its content is objective and at the same time it is recognized by the investigating authority in relation to the circumstances of a particular criminal case. In connection with the last situation in the forensic literature, attempts have been made to differentiate the goals of crime investigation (planning).

The principle of validity implies the existence of a sufficient basis for all that is outlined in the plan, based on the information available to the investigating authority. At the same time, the source of such information, for example, in the investigation of crimes committed using banking technologies, can be materials from the criminal case, operational services, government agencies, credit organizations, etc.

**2.  Resources**

The principle of planning dynamism, on the one hand, consists of the continuity of planning and ensuring the necessary speed, mobility and flexibility of planning as new information about the crime is received, the conditions and conditions of the investigation change. On the other hand, it is a manifestation of the pattern of development of the investigative version. In the process of checking investigative versions, new information about the facts appear, new assumptions about the circumstances of the crime are verified, some versions disappear, others appear, and this happens before the investigation is completed, until the truth of the case is established.

The logical dynamics of the investigation will inevitably cause dynamics in the planning, constant updating and changing the plan of the investigation, taking into account the newly received information. Thus, even the most perfect, deepest, a prospective investigation plan is undergoing continuous adjustment. It does not at all follow that when drawing up the initial plan of the investigation, one can neglect the requirements of the comprehensiveness and depth of analysis of the materials received, the detailed development of investigative versions, planned measures, etc. counting on the fact that the plan is "unstable" and will be changed and supplemented (Dean, G., Filstad, C., & Gottschalk, 2006).

The principle of dynamism of planning obliges the investigating authority to timely make the necessary additions and amendments to the plan of the investigation, taking into account newly received information and changes in the investigative situation. detailed development of investigative versions, planned events, etc. counting on the fact that the plan is "unstable" and will be changed and supplemented. The principle of dynamism of planning obliges the investigating authority to timely make the necessary additions and amendments to the plan of the investigation, taking into account newly received information and changes in the investigative situation. detailed development of investigative versions, planned events, etc. counting on the fact that the plan is "unstable" and will be changed and supplemented. The principle of the dynamism of planning obliges the investigating authority to timely make the necessary additions and amendments to the plan of the investigation, taking into account newly received information and changes in the investigative situation.

The reality of planning assumes that the investigation authorities have the necessary resources at their disposal. All planned procedural and other actions (measures) and / or their complexes should be feasible, planned taking into account the specific conditions and capabilities of the investigation body, which are predetermined by the availability of appropriate resources? In the investigation of crimes committed using banking technologies, these may be: the presence of a sufficient number of operational employees, as a rule, units of the FS ENP, relevant specialists, the possibility of forensic examinations, primarily forensic economics, computer technology, the possibility of using information in the investigation process resources (both computer hardware and related software products) of temporary resources, technical means (e.g. motor vehicles). Otherwise, the investigation planning process will be divorced from the specific circumstances of the criminal case.

In these conditions, the inevitable: errors in determining the only correct the direction of the investigation, distraction of the investigation body to useless measures, loss of the optimal pace of work in a criminal case. The reality of planning is also expressed in the practical feasibility of the planned activities, the possibility of observing their deadlines.

**3.  Develop a Plan**

The first stage of planning is to analyze the information available to the investigating authority due to the investigative situation at the time planning began.

The sources of information about the investigated event may be various documents contained in the criminal case materials at the time of planning. The volume of such sources depend on the stage (s) of the investigation. So, at the initial stage of the investigation (immediately after the decision to institute criminal proceedings), the sources of information for planning the investigation may be:

* Reports of a crime (statement of crime, confession, report on the detection of evidence of a crime, media reports, etc.);
* The protocol of explanations of eyewitnesses of the incident, victims, etc .;
* acts of departmental official audits, tax audits, documentary accounting audits (inspections);
* materials obtained in the course of administrative proceedings (for example, a protocol on an administrative offense, explanations of persons in respect of which an administrative offense was conducted, testimonies of victims, witnesses, expert opinions, other documents (copies thereof), material evidence, etc. .);
* results of operational investigative activities;
* materials submitted by competent authorities of other countries;
* regulations governing the sphere of public relations that have been subjected to criminal assault. It should be borne in mind that the legislation is changing dynamically, so you should carefully compare the time of the investigated event with the period of the validity of certain regulatory acts;

 In addition to the main plan, and often even before its formation, the investigating authority, especially in complex and / or multi-episode cases, develops supporting planning documents:

1) Cards ("personal accounts") on suspects (accused), where episodes of criminal activity is introduced in which the suspect (accused) took part, and data collected for each episode confirming his guilt. “Personal accounts” are separate cards (sheets of paper) compiled separately for each accused, and a card file is a collection of all “personal accounts”;

2) Chess sheets ("chess"): a combination of a graph with a description, a set of "personal accounts", deployed on a single sheet, where each horizontal column represents one of the "personal accounts". The chess sheet gives clarity to all the data collected on the case. “Personal accounts” and “chess” can be compiled by the investigating authorities before the investigation versions are put forward, in the process of studying primary information as a means of analyzing and systematizing (logical ordering).

3) various schemes and graphs reflecting the criminal ties of the accused, the movement of material assets and money, document flow, the organizational structure of enterprises and associations, the territorial location of individual organizations, etc.

**4. Step 4**

All additional forms of planning help to better navigate the case materials, unload the memory, give greater visibility to the collected evidence and upcoming actions are a kind of accumulative fund, an information base for the investigation as a whole and its planning in particular. The modern level of theoretical ideas about planning an investigation of crimes allows introducing into scientific and practical use the concept of “working documentation”, which should be understood as the entire volume of documents that accompany the investigation of crimes, but which are not procedural, evidence, or other documents that are based on Criminal Procedure Law attached to the materials of the criminal case (Yinghui, 2000). These documents should include:

Orders and instructions on the creation of SOGs and investigative teams and changes in their composition;

* criminal investigation plans and programs;
* Schemes: investigated criminal activity, preliminary investigation, relations between members of a criminal group (criminal communities, etc.), the movement of criminal capital, banking technologies that were used to commit crimes, etc.;

If the investigation of crimes is carried out by SOG, then planning is carried out by a group method, i.e. the head of the SOG, with the participation of all its members draw up a general plan of investigation of the criminal case, and, in addition, each member of such a group draws up his own, individual plan of investigation.

It seems that the triad of “planning, programming, algorithmization” can be considered as a single organizational element of private forensic techniques in the modern sense of the latter. Under the investigation program, we can understand the data intended to manage specific components of the system - the process of investigating crimes, processing information in order to implement a specific investigation algorithm. The latter, in turn, is an exact instruction to the investigating authority (SOG members), a certain sequence of procedural and other actions (measures) or their complexes to achieve the goal in a finite number of steps. Thus, the plan of investigation contains the program and algorithm of the investigation, as well as other data of an informative nature, allowing the most effective investigation of crimes (for example, indicating the number of the criminal case, the date of the start of the investigation, a brief plot of the case, investigative versions, tasks of the investigation, target dates for the stages of the investigation, etc.). At the same time, the investigation program in some cases, as was noted, it is advisable to set out separately, which optimizes the process of planning the investigation and allows for the multi-episode and / or most complex criminal cases to effectively organize the production of the preliminary investigation.

**5. Toyota Motor Corporation**

*“Toyota Motor Corporation is a Japanese multinational automobile manufacturer headquartered in Toyota, Aichi, Japan. In 2017, Toyota's corporate structure had 364,445 employees worldwide and, as of September 2018, was the sixth-largest company in the world in terms of revenue.*

*“The Moscow representative office Toyota Motor Corporation, Japan recommends TerraLink as a reliable partner”.* The company "TerraLink" provides after-sales service of the local network, the supply of computer equipment and software to Toyota Company. In early March 2018, the Japanese auto giant Toyota announced the creation of a new unit that will focus on the development of unmanned vehicles. Its employees will create “fully integrated, production-friendly drone driving software, (Yamada, 2013).”

 6. **Organizational structure**

From April 1, 2013, Toyota Motor Corporation’s automotive business will be divided into 4 main structural divisions, in order to more clearly distribute areas of responsibility and make quick decisions. The changes were designed to enhance Toyota’s competitive advantage and contribute to the implementation of sustainable growth strategies at the global level. New organizational and managerial structures were proposed after a thorough analysis of business methods and management decision-making mechanisms in the company.

**Organizational Structure**

**Directors**

**Manager sales and marketing**

**Manager finance**

**GM after sales**

**Manager body and paint**

NAWEED HADI

**CR Manager**

MEHMOONA

**Manager parts**

**Admin sales Coordinator**

**Deputy Manager sales**

**Service manager**

Paint Technicians

KHURSHID

MEHRAJ

AZHAR

ADIL

SHAFEEQ

NADEEM

**Dent Technicians**

**TANVEER**

**ABID (PEYA)**

**ASIF**

**WAQAS**

Manager Parts

RASHID

Manager Body & Paint

SARDAR ASIF

NAWEED HADI

**CR officer**

**Dent Technicians**

**Paint Technicians**

NAWEED HADI

**Service Advisor**

**Assistant manager**

**Cashier**

**Warranty advisor**

**7.CIA**

The United States Central Intelligence Agency (CIA) is a department of the US the federal government and the main foreign intelligence and counterintelligence agency in the United States.

*“Confidentiality, integrity, and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity, and confidentiality) to avoid confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security. PHI is any demographic information that can be used to identify a patient)”.*

**8. Cyber threats**

Toyota is the target of a new cyber attack after an initial intrusion reported in late February 2019. Several Japanese affiliates are affected this time. Attackers could potentially access data from 3.1 million customers

The automaker Toyota revealed on March 29, 2019, that it was the victim of a security breach impacting several of its Japanese subsidiaries. The personal data of 3.1 million customers are potentially affected (Yamada, 2013).

**9. TWO ATTACKS IN TWO MONTHS**

This is the second flaw reported by the manufacturer in two months. A first attack had targeted Toyota's Australian division in February. The same criminal group appears to be behind both attacks, according to FireEye experts. The Australian branch could have served them to have access to the servers of the Japanese divisions.

Toyota has not yet revealed the nature of the data that hackers could access, the investigation is still ongoing. The company is looking for the moment to determine if they have been downloaded. She nevertheless stated that the financial information of the customers was not concerned, because not stored on these servers. The manufacturer has also announced measures to strengthen its global security.

Toyota: victim of two cyberattacks in 5 weeks

* At the end of February, the Australian division of automaker Toyota was the victim of a cyber attack targeting the personal data of users.
* In late March the Japanese brand reported a similar intrusion into its computer system.
* Hackers had access to data from more than 3 million consumers of the automobile builder.
* This the attack has indeed affected a large number of subsidiary fu Toyota group such as: Tokyo Tokyo Sales Holdings, Tokyo Tokyo Motor or Lexus Koishikawa Sales.

**9.1 Benefits**

Toyota is determining exactly what information the hackers had access to and how many people were affected by the attack. However, the group has announced that no financial information has been compromised because it is not stored on the affected server. According to FireEye's experts, both attacks were allegedly perpetrated by the same cybercriminal group. Their intrusion into the Australian branch may have allowed them to break into the servers of the Japanese division.

Toyota has announced important steps to strengthen its global security and reassure consumers. For this, an internal audit will be conducted on all of the group's IT servers. Toyota Financial Services selects Ivanti Patch for Endpoint Manager (powered by Landesk), Ivanti Device Control (powered by Heat) and Ivanti Application Control (powered by AppSense), with the following key benefits:

* Significant reduction in patching time
* Reduced risk of errors in updates
* Previous error correction
* Enhanced mobile device security (USB sticks)
* Mobile RGPD compliance support Helps meet
* security audits annually
* White List and Contextual Blacklists and Privilege Management.

Present in around 40 countries, Toyota Financial Services offers its clients a full range of financing and related services through its dealer network. As an international company, Toyota Financial Services supports its IT strategy on global solutions for all its locations, while maintaining a certain autonomy for each country, according to their local issues and constraints.

Thus, if networks, remote access, links and inter-sites and messaging are global, the core network, storage and virtualization systems, office tools or some business solutions are entirely within the IT competence of each in the context of global objectives, including security.

In response to these safety guidelines from the Japanese parent company, the IT France team has, for several years, processed patching manually, aided by a few sporadic tools that did not meet the needs of managing updates on the Internet. Entire IT perimeter administered locally. Because unfortunately, when patches are applied manually, it happens that malfunctions occur, preventing the update of some components. "This is a problem we had with VMware Tools," recalls Pierre NG, Toyota Financial Services' Information Systems Security Manager.

**10. Solution**

As of March, the solution is deployed on almost 300 devices spread over 2 sites: 20 physical servers, more than 150 virtual servers, 20 laptops, 100 virtualized workstations, etc.

In addition, Toyota Financial Services France also uses Ivanti's Application Control solution to complete the security of its IS, against the risks of Zero-Day operations or the execution of unauthorized applications, by associating whitelists. dynamic and fine management of privileges. To reinforce this precautionary approach, the Ivanti Device Control solution enables Toyota Financial Services to quickly identify each mobile device (including USB keys) and to make it more secure, so that no application can be installed or run from scratch. an unknown mobile device, thus reducing the potential attack surface of the enterprise.

**Recommendations for Toyota Motors**

* Toyota is not at its first failure. Already February 12, the car company had to recall 1.9 million vehicles of its model Prius. "This company should focus the quality and treat it before it represents a risk for the consumer.
* In parallel, the recurrent security audits made it necessary to have better control of the applications, while, in particular, to meet the new obligations of the RGPD, the use of mobile devices and USB keys should identify and encrypt became mandatory.
* For RAV4, Land Cruiser, and Hilux models, the driver's airbag may no longer work. But the user would still be informed via the indicator light on the dashboard. As for the seats of the Yaris and Urban Cruiser, they will not lock, which would cause their displacement back and forth in case of shock.

**References**

Maguire, M. (2003). Criminal investigation and crime control. Handbook of policing, 2, 430-464.

Dean, G., Filstad, C., & Gottschalk, P. (2006). Knowledge sharing in criminal investigations: an empirical study of Norwegian police as value shop. Criminal justice studies, 19(4), 423-437.

Yinghui, S. (2000). An Approach to the Technical Investigation in the Criminal Procedures [J]. CASS JOURNAL OF LAW, 3.

Greenwood, P. W., & PETERSIUA, J. (1975). THE CRIMINAL INVESTIGATION PROCESS VOLUME I: SUMMARY AND POLICY IMPUCATIONS.

Leo, R. J. (1982). An Update of the Japanese Automobile Export Restraint. Brook. J. Int'l L., 8, 159.

Yamada, K. (2013). U.S. Patent No. 8,536,810. Washington, DC: U.S. Patent and Trademark Office.

Shu-jun, J., & Hui, L. (2013). Analysis on the Lean Production about Electronic Assembly Line. Control Engineering of China, S1.